TOG Mind

Confidentiality Policy

Revision History
Document/Policy Title: TOG Mind Confidentiality Policy

Document Control	
Document Title:	TOG Mind Confidentiality Policy
Document Type:	Policy
Author:	Claire McGrath
Issue Date:	August 2022
Date of Executive Committee:	1 August 2022
Name of Executive Lead:	Cheryl Eastwood
Version Number:	3
Review Date:	August 2025

Previous Version	**Significant Changes from previous version**	**Author**	**Date**
1	Full review	Claire Shuttleworth	August 2018
2	Updated with new policy template	Claire Shuttleworth	June 2020
3	Full review for relevance and accuracy, included Caldicott principles, relevant legislation	Claire McGrath	July 2022

1. Introduction & Background

The purpose of this Confidentiality Policy is to set out the principles that must be considered by all who work within Tameside Oldham and Glossop (TOG) Mind. All staff are bound by a legal duty of confidence to protect the personal information that they encounter during their work and need to be aware of their responsibilities legally and in accordance with TOG Mind policies. In completion of standard organisational practices, TOG Mind staff and volunteers process significant quantities of information, in multiple formats including digital, analogue, and verbal. Commonly, this information may be the personal data of beneficiaries, suppliers, staff, volunteers, supporters/campaigners, donors and trustees. Information may also include sensitive organisational documents that are not publicly available and may have adverse implications for the charity if disclosed.

2. Purpose and aims of this policy

The overriding aim of this Policy is to protect and promote the best interests of individuals and TOG Mind, and any question concerning confidentiality should be answered by reference to this principle.

<u>When working with TOG Mind you must:</u>

- Treat all personal data and sensitive organisational information as confidential to TOG Mind

- Comply with the law regarding the protection and disclosure of information (including the Data Protection Legislation) and our policies, specifically our Data Protection Policy and Information Sharing Policy.

Any breach of this Policy could have very serious consequences for an individual or for TOG Mind and will be treated as a serious disciplinary matter.

3. Legal Framework

This Policy is designed to be read and considered in conjunction with national legislation relating to confidentiality in Health and Social care, as well as local TOG Mind-related policies. This policy has been developed in line with the following legislation and guidance:

- Common Law Principle of Confidentiality
- Caldicott Review, 2013
- The Human Rights Act 1998
- The Care Act 2014
- The Health and Social Care Act 2015
- The Data Protection Act 2018
- UK GDPR
- TOG Mind Data Protection Policy
- TOG Mind Information Sharing Policy
- TOG Mind Privacy and Cookies policy

- TOG Mind Children's safeguarding policy
- TOG Mind Adult Safeguarding policy
- All other applicable TOG Mind policies and procedures concerning information governance

4. Scope

4.1 The policy and procedures in this policy are applicable to staff, volunteers, trustees and contracted third parties. If you are in any doubt about the application of this Policy, please seek guidance from a manager, the Data Protection Officer or the Caldicott Guardians.

4.2 If a situation arises where there is a potential conflict in applying this policy within a situation, please seek guidance from a manager. If necessary, managers should seek guidance from the Data Protection Officer (DPO), Senior Information Risk Officer (SIRO), or Chief Executive Officer (CEO).

5. Roles and Responsibilities

5.1 **The Executive Committee and the Chief Executive** have overall strategic accountability for confidentiality, including the maintaining of this policy and relevant frameworks. They are responsible for assuring that confidentiality is managed appropriately within the Charity. The Executive committee and CEO delegate responsibility to the Senior Information Risk Owner and Caldicott Guardians

5.2 **Caldicott Guardians** act as the 'conscience' of Tameside Oldham and Glossop Mind. Within this role, they facilitate information sharing and advise on the lawful and ethical processing of information. TOG Mind have 2 Caldicott Guardians with leads for Children and Adults.

5.3 **Senior Information Risk Owner (SIRO)** has responsibility for compliance with legislation and national policy in relation to the security of personal identifiable information (PII).

5.4 **Data Protection Officer (DPO)** provides advice to the organisation and employees on data protection issues which can include confidentiality issues. These issues are to be reviewed in collaboration with the Caldicott Guardians to ensure compliance with data protection law.

5.5 **The HR team** is responsible for ensuring that confidentiality clauses are contained within all contracts and the employee handbook. The HR Team also issue and process employee confidentiality agreements. They are also responsible for ensuring confidentiality is included in inductions for all staff.

5.6 **Line Managers** will be responsible for ensuring that all TOG Mind staff are compliant with this policy and have completed all relevant training modules. Line managers have a responsibility to ensure any incidents or policy breaches are reported in line with the organisation's Incident Policy and Data Breach Policy.

5.7 **All staff** and anyone performing duties on behalf of TOG Mind have responsibilities for confidentiality on a day-to-day basis. All staff should be aware that their employment contracts include a confidentiality clause, and they are required to participate in induction and training in relation to confidentiality.

6. Caldicott Principles

6.1 All personal data and confidential information about TOG Mind, our partners and other third-party organisations must be kept and handled confidentially, whether the information has been received formally, informally or discovered by accident – anything seen or overheard accidentally is still personal data.

In summary, this includes:

- Any information which relates to or is about an identified or identifiable individual (PII) i.e., their name linked with any other information about them (address, telephone number, etc).
- Anything else provided to us in confidence by third parties and that is not a matter of public record
- Sensitive organisational information that could be used to damage TOG Mind such as unpublished business plans/strategies, system access details or business continuity plans.

The Caldicott principles are intended to apply to data collected for the provision of health and social care services. The principles are relevant for all confidential information and TOG Mind staff are expected to consider the principles in relation to the collection and use of any personally identifiable or confidential information.

Principle 1: Justify the purpose(s) for using confidential information
Every proposed use or transfer of confidential information should be clearly defined, scrutinised, and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary
Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information
Where the use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strictly need-to-know basis
Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities
Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patients and service users.

Principle 6: Comply with the law
Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators, and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used
A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

7. Handling Confidential Information

7.1 All personal data should be treated in the strictest confidence and in accordance also with our Data Protection Policy. Personal data should only be disclosed outside the Charity in line with our Information Sharing Policy. The Privacy and Cookies Policy sets out the procedure for dealing with requests from individuals for their own information as well as Subject Access Request guidance documents

7.2 <u>General Rules for Handling Information</u>

When handling personal data and other confidential information of TOG Mind, its partners, and other third-party organisations, always follow a few simple rules:

- Even in the most innocent of conversations, do not discuss any part of your work that could cause either an individual or TOG Mind embarrassment or harm
- Be aware of who else may be listening, particularly in areas open to the public
- All staff should clear their desk at the end of the day per the organisation's Clear Desk Policy, ensuring that any confidential information is locked away
- Always lock your computer screen if you leave your desk unattended and log out completely when you have finished for the day, per the organisation's Clear Desk Policy
- Never leave confidential information unattended, either put it in an envelope marked confidential or lock it away. If someone comes near you while you are working, discreetly cover the material or ask the person to go away
- If you need to take sensitive documents away from the office, seek permission first
- Do not read or process confidential documents on public transport
- Do not leave confidential documents unattended in cars or public places
- When it is absolutely necessary to store information at home, ensure this is done so securely
- Check communication preferences with individuals to ensure personal sensitive information is sent in the most appropriate and confidential method for the person
- Do not repeat personal information over the phone, ask the person to repeat if you are unsure
- Explain to individuals why the information you are collecting is needed and how it will be used
- Ensure individuals are aware of TOG Mind Privacy and Cookies Policy and the Privacy notice displayed in buildings

7.3 <u>Ensure that any personal data you record is:</u>

- **Factual and relevant.** Keep expressions of opinion to a minimum and make sure they are fully justifiable on the basis of the factual information
- **Accurate.** Wherever possible, take notes during interviews and conversations and use the person's own words. Check the record with them if possible. Where appropriate, ask for and examine supporting documents and record this on the file

- **Comprehensive and clear.** Another staff member might have to form a judgement from the information and the person concerned may wish to read it

7.4 Handling Incoming Information

- All external post should be opened at reception and checked if addressed to the organisation. The post should then be distributed accordingly subject to the following:
- Internal post marked confidential should be passed to the addressee unopened
- If anything of a confidential nature is not in an envelope, put it in a sealed and appropriately marked envelope before passing it to the addressee
- If you open confidential correspondence by mistake, reseal it or use a new envelope and write your name and 'opened in error' on the outside before forwarding it to the addressee. Proceed to log a data breach incident per the organisation's Incident Policy.

7.5 Typing and Administration

- The administration, typing, printing, photocopying, faxing, and filing of confidential information must only be carried out by employees or volunteers who are familiar with TOG Mind confidentiality procedures.
- The following precautions should always be taken:
    - Take care to securely destroy all unused rough work and any spare copies using the document destruction and disposal facilities provided in our offices
    - When photocopying, utilise a security pin so you only print confidential information when you are able to collect it immediately – this is the 'secure printing' function.

7.6 Working with computers

- No discs, CDs or other portable storage media should be used to store personal data unless encrypted and unless authorised by TOG Mind's IT Support and a Director.
- All/any personal data stored on laptops to undertake outreach or remote clinical services should be encrypted.
- Computers should be locked, or users should log out to prevent access if computers are left unattended for any length of time, per the organisation's Clear Desk Policy.
- When using e-mail addresses, external recipients should not be grouped unless permission has been obtained
- The Bcc facility on e-mail should not be used as a mechanism for sharing or distributing personal data.

7.7 Keys

- All keys to TOG Mind properties, filing cabinets and desk drawers must be kept as secure as possible and where appropriate only issued to staff who require them. Spare keys should be kept in a locked place. Do not keep keys in unlocked drawers.

8. Information Obtained by Beneficiaries/Participants

8.1 Beneficiaries involved in group work/peer support activities are likely to be aware of personal data about other beneficiaries and should be made aware of the need to respect their right to privacy.

8.2 Participants involved in group work/peers support activities will be asked to participate in developing a group agreement that outlines their responsibilities around disclosures from other members of the group to ensure all members feel safe and personal details remain confidential

8.3 TOG Mind will make participants aware of their responsibilities under these circumstances and they are responsible for ensuring they comply.

9. Access to Confidential Information

9.1 All employed staff, sessional workers and volunteers must sign a confidentiality agreement before being given access to TOG Mind information assets. For paid staff, this agreement forms part of their contract of employment (See Appendix A). For volunteers, it is covered by TOG Mind's volunteer confidentiality pledge (See Appendix B). Relevant employees with privileged access to systems and information must have signed an agreement covering a higher level of confidentially and responsibility for data protection and data security.

10. Sharing with Third Parties

10.1 External agents and contractors who process personal data and other confidential information on behalf of TOG Mind must be made aware of TOG Mind's information governance requirements; what they can and cannot do, and who they should contact if things go wrong prior to them being given any access to TOG Mind's information assets.

10.2 All agents and contractors who have a service level agreement with TOG Mind, will adhere to the terms set out in the SLA which includes obligations around Data Protection legislation and confidentiality. Within the SLA process, TOG Mind will also complete a due diligence process to ensure that providers/sub-contractors have appropriate policies and procedures in place that adequately cover confidentiality, security and information governance arrangements

11. Disclosing Personal/Confidential Information

11.1 There is no absolute right to confidentiality in law and absolute confidentiality cannot, therefore, be guaranteed. In a circumstance where confidentiality cannot be adhered to, TOG Mind will endeavour to communicate with clients in advance of any disclosure to ensure openness and transparency. There may be occasions where the communication of the disclosure may have the potential to cause harm to the client or others, in these circumstances TOG Mind may disclose information without informing clients beforehand. There are circumstances where TOG Mind will be bound to share personal information in compliance with the law and public protection under a statutory duty, as set out below:

11.2 Clients at risk from harm to self and others

TOG Mind owes a duty of care to all its clients; as such, where a client is acting, or is likely to act, in a way that could cause serious harm to him or herself or others, the Charity will, if need be, act on behalf of the client.

11.3 Safeguarding adults at risk

TOG Mind is legally obliged to safeguard adults at risk as defined in The Care Act 2014. An adult at risk is a person who has care and support needs and is, or is at risk of, being abused or neglected and unable to protect themselves against the abuse, or neglect or risk of it because of those needs. (Also See Adult Safeguarding Policy)

11.4 Child protection

TOG Mind is obliged to disclose any information in the interests of safeguarding children, as set out in The Children Act 2004, Working Together to Safeguard Children 2018 (See also Safeguarding Children Policy)

11.5 Legal obligation

1. TOG Mind is bound by offences in the Prevention of Terrorism Act 2005 which refers to the information given on any planned act of terrorism or where there is cause for concern regarding terrorist activities.

2. TOG Mind is bound by offences in the Drugs Trafficking Act 1994 and any information in regard to the money laundering regulations 2019, or where there is cause for concern regarding this type of criminal activity.

3. In the event of a court case, the judge has the power to subpoena a client's notes, or request that a service report is provided as evidence for the case. In these instances, TOG Mind must comply. Prior to sending these records, the Caldicott Guardian would be consulted and they would review the records prior to providing them to the court.

If staff have any concerns about disclosing information, they should seek support from their line manager and if further guidance is needed you should contact datarequest@togmind.org. Guidance and advice will be sought from the TOG Mind's Data Protection Officer and Caldicott Guardians.

11.6 Managing a breach of confidentiality

If accidental disclosure occurs, the responsible TOG Mind manager should take swift action to minimise the damage. They should find out who knows about the incident, talk to them, and remind them of their duty to maintain confidentiality. Only where there are legitimate concerns that informing the client/service user will increase the risk to both themselves and others, the client in these instances will not be informed.

The breach must be reported in line with TOG Mind's Data Breach Guidance Policy. If there is the potential for adverse publicity, then the Chief Executive Officer must be alerted. In any event, the Caldicott Guardian must be informed of all confidentiality breaches even if they have already taken place.

All staff should help to prevent accidental disclosures from occurring by regularly pointing out that certain information is confidential, reporting near misses through the TOG Mind incident system to support continued understanding and learning.