Confidentiality Policy

1. Introduction & Background

1.1 During the course of everyday working, Burton and District Mind staff and volunteers handle a great deal of information, in both paper and electronic formats. Some of this is the personal data of beneficiaries, suppliers, staff, volunteers, supporters, donors and trustees and is covered by our Data Protection and information Security Policy. Information about Burton and District Mind and its work is also sensitive and confidential and could, if disclosed, have adverse implications for the Charity.

1.2 Burton and District Mind aims to strike a balance between encouraging openness, avoiding unnecessary secrecy, and ensuring individual privacy is respected.

1.3 Most breaches of confidentiality happen through lack of thought or consideration of the possible consequences, or a lack of private or secure facilities. The best protection against breaches of confidentiality is to keep to a minimum the number of people who have access to sensitive information. Anyone worried or distressed by something they hear or read should seek guidance and support from a member of the senior management team.

2. Scope

2.1 The policy and procedures in this policy (referred to as this Policy) are applicable to staff, volunteers, trustees, and clients. If you are in any doubt about the application of this Policy, please seek guidance from the Chief Officer.

2.2 This Policy is designed to work with and support various codes of professional conduct that are applicable to some of the work undertaken by the Charity as well as to support guidance used by the Charity on safeguarding children and vulnerable adults, data protection, and use of information technology. It should be read in conjunction with the Data Protection and Information Security Policy, Retention schedule, Safe Haven Procedure, as well as the Consent to disclose form and counselling contract.

2.3 If a situation arises where there is a potential conflict between the codes and this Policy, please seek guidance from the Chief Officer.

3. Policy Statement

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

3.1 When working with Burton and District Mind you must:

- Treat all personal data and sensitive organisational information as confidential to Burton and District Mind
- Comply with the law regarding the protection and disclosure of information (including the Data Protection Legislation) and our policies, including our Data Protection and Information Security Policy.

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

4. Information to be kept confidential

4.1 All personal data and confidential information about Burton and District 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.

4.2 Broadly, this includes:

- Any information which relates to or is about an identified or identifiable individual 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 cause damage to Burton and District Mind

5. Handling Confidential Information

5.1 All personal data should be treated in the strictest confidence and in accordance also with our Data Protection and Information Security Policy. Personal data should only be disclosed outside the Charity in line with this policy and a data request must be made in writing.

5.2 Your work is likely to bring you into contact with information that is personal to someone or organisational information that is not yet ready for distribution. Anyone worried or distressed by something they hear or read should seek guidance and support from the senior management team.

5.3 When handling personal data and other confidential information of Burton and District 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 Burton and District Mind embarrassment or harm.

- Be aware of who else may be listening, particularly in areas open to the public
- Get into the habit of checking and clearing your work area and locking your desk and filing cabinets before leaving at the end of each day. It is acceptable to leave some work out, but lock away anything confidential or even for limited circulation
- Always lock your computer screen if you leave your desk unattended and log out completely when you have finished for the day
- 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 step 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 Store them securely at home and do not show them to other household members
- Remember that information in the wrong hands can cause a lot of damage and unnecessary stress

5.4 In discussions or meetings

- Only disclose information that is relevant
- Do not discuss personal information about another person
- Do not disclose the name of a person making an allegation about someone else without the complainant's consent
- Refer to beneficiaries by reference codes (e.g. initials) in management meetings

5.5 When entering into correspondence with an individual that will contain personal data (including, for example, sensitive information such as health data), you should:

- Check with the person concerned that they can be written to at their home address or make arrangements for letters to be collected or sent elsewhere
- Check whether correspondence should be marked private and confidential

5.6 When collecting and/or recording information about a person:

- Offer a private interview
- If the conversation is over the telephone and someone else might hear, do not repeat aloud any personal information. If necessary, ask the person to say it again
- Explain first why the information is needed and how it will be used and obtain their consent if required. If we need to collect it for legal or other purposes, we must tell them that.
- We should give them a copy of our privacy notice or refer them to the privacy notice on Burton and District Mind's website for more information.

5.7 When collecting sensitive personal data (for example, health information) in many cases we will need to have explicit consent –this can be an oral or written statement. We should also explain:

- Who will have access to it
- The implications of not giving the information
- Any special procedures for protecting particularly sensitive information
- If the individual does not agree, do not record or pass on the information. Explain this and its implications to the person
- Do not ask questions that are not relevant

5.8 Ensure that any personal data you record is:

- 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 necessary. 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

5.9 Handling incoming information

- All external post should be opened in the main office.
- 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

5.10 Typing and administration

The administration, typing, printing, photocopying, and filing of confidential information must only be carried out by employees or volunteers who are familiar with Burton and District Mind confidentiality procedures.

The following precautions should always be taken:

1. Take care to securely destroy all unused rough work and any spare copies.

2. When photocopying, do not let anyone else read the documents, make only the required number of copies and check that nothing is left in the machine afterwards.

5.11 Working with computers

- No portable storage media should be used to store personal data unless encrypted and unless authorised by Burton and District Mind.
- 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.
- All user accounts must be protected by strong passwords and passwords to be held securely by the owner. Passwords should be changed every 4 months or if you think someone else might know your password.
- When using e-mail addresses, external recipients should not be grouped unless permission has been obtained or blind copied
- Unless it is necessary no personal data should be transferred via email, if there is an occasion where this is required it should either be encrypted or password protected.
- When paid or unpaid workers leave the organisation, all Burton and District Mind data must be deleted from their laptop.

5.12 Keys

- All keys to Burton and District Mind properties must be kept securely with spare keys kept in a key cabinet or drawer that is kept locked. Do not keep keys in unlocked drawers.
- Filing cabinets and desk drawers with confidential information should be kept locked and keys kept securely with spare keys kept in a locked key cabinet. Do not keep keys in unlocked drawers.

6. Access to sensitive information

6.1 Staff will generally have access to all information that they genuinely need to know to carry out their work, and are under a duty to respect the confidentiality of all personal data held by Burton and District Mind.

6.2 Staff should have explained or made privacy information available to the individual to explain the purpose of recording the personal data, how that information will be used and whether it will be shared with any third parties when they collect the information. If this causes concern, special arrangements for recording and access will be made where possible. If concerns cannot be allayed it may be impossible for Burton and District Mind to undertake a particular activity for a given individual.

7. Information obtained by beneficiaries

7.1 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.

7.2 Beneficiaries involved in group work/peers support activities will be asked to sign or confirm their agreement to a participation agreement prior to their involvement outlining their responsibilities and disclosure risks from other members.

7.3 Burton and District Mind will make beneficiaries aware of their responsibilities under these circumstances and they are responsible for ensuring they comply with agreed ground rules for their activity.

8. Access to confidential information

8.1 All employed staff, sessional workers and volunteers must sign a confidentiality agreement before being given access to Burton and District Mind information assets. For paid staff this agreement forms part of their contract of employment (See Appendix A). For volunteers it is covered by Burton and District Mind's volunteer confidentiality pledge (See Appendix B).

9. Sharing with third parties

9.1 External agents, partners and contractors who process personal data and other confidential information on behalf of Burton and District Mind must be made aware of Burton and District 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 Burton and District Mind's information assets.

9.2 All agents, partners and contractors in receipt of Burton and District Mind confidentiality information should complete and sign a confidentiality agreement at the outset of the contract being established.
A standard contract is set out at Appendix D.

9.3 Burton and District Mind senior managers responsible for contracting with third party organisations where access to Burton and District Mind's information assets is required should undertake a due diligence check and risk assessment to establish the adequacy of the third party's confidentiality, security and information governance arrangements.
A proforma is set out at Appendix C.

10. Managing a breach of confidentiality

10.1 If accidental disclosure occurs, the responsible Burton and District Mind senior Manager/Officer 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.

10.2 The breach must be reported in line with Burton and District Mind's Information Breach reporting form.

10.3 All staff should help to prevent accidental disclosures occurring by regularly pointing out that certain information is confidential and checking that people have understood.

11. Disclosure

11.1 Disclosure of personal data and other confidential information should only be made in accordance with Burton and District Mind's Information Sharing procedures and Consent to Disclose form.

12. Disposal

12.1 When no longer required, all personal data and other confidential information, including computer printouts, will be securely shredded or destroyed.

13. Roles and responsibilities
13.1 The CO and the board of trustees is responsible for gaining assurance that confidentiality is managed appropriately within the Charity and that adequate resources are made available to implement this Policy.

13.2 The CO is responsible for ensuring that all confidential information processed by the charity is handled in line with this Policy and associated procedures and for providing assurance of such to the trustees.

13.3 The individual in charge of GDPR compliance is responsible for ensuring that access to confidential information is audited in line with the Burton and District Mind's audit procedures.

13.4 The individual in charge of GDPR compliance is responsible for providing advice in relation to this Policy.

13.5 The CO is responsible for ensuring that confidentiality clauses are contained within all contracts in accordance with the Confidentiality Agreements Procedure and that confidentiality training is included in corporate inductions.

13.6 Senior Managers/Officers will be responsible for ensuring that all Burton and District Mind staff working in a service delivery role have read this Policy, and understand the Information Sharing procedures and are working to the required

standard. They will ensure that a high standard of record keeping is maintained by conducting regular audits and will provide annual eLearning training for staff.

13.7 All Burton and District Mind staff with access to confidential information have responsibilities to ensure that they comply with this Policy and with any guidance subsequently produced.

Adopted 27 Jan 2022

Appendix A:

Staff contract clause Confidentiality and Data Protection –

Much of the information relating to the Charity and its services, those that receive services, other employees or volunteers, is confidential.

It will usually be clear when information is confidential but you should be aware that, due to the sensitive nature of the Charity's work, certain facts and information could fall within this category which may not be treated as confidential in other organisations.

Any employee, who is in doubt about whether particular information is confidential, should seek the advice of his/her senior Manager/Officer.

You may not during or after the termination of your employment disclose to anyone other than in the proper course of your employment or where required by law any information of a confidential nature relating to the Charity or its business, staff, volunteers, Beneficiaries or customers.

Breach of this clause may lead to dismissal without notice. Guidance on standards expected can be found in the confidentiality policy.

The Charity is registered in accordance with the requirements of the Data Protection Bill 2018.

You are required at all times during your employment to comply with the provisions of the Data Protection Bill 2018 and with any policy introduced by the Charity to comply with Data Protection Legislation, in particular with the Burton and District Mind Data Protection and Information Security policies and procedures.

Signed ..... Dated .....

Appendix B:

Volunteer Confidentiality Pledge –

This form is an agreement for individuals volunteering for Burton and District Mind, outlining the requirement for the security and confidentiality of data and information relating to beneficiaries, members, supporters, staff and volunteers and the work of Burton and District Mind.

Mind Burton and District

During your period of volunteering with Burton and District Mind you may acquire or have access to personally identifiable and sensitive organisational information, which must not be disclosed to any other person, unless in pursuit of your duties, as detailed in the volunteering agreement between Burton and District Mind and yourself.

Confidential information includes all information relating to the work of Burton and District Mind and its beneficiaries, members, supporters, staff and volunteers. The General Data Protection Regulation (EU) 2016/679 and the UK laws that implement it (Data Protection Legislation) regulate the use of all personal data and includes electronic and paper records of identifiable beneficiaries, members, supporters, staff and volunteers.

Mind is registered in accordance with the Data Protection Legislation and is also bound by the Information Governance standards applicable to all NHS and partner organisations.

If you are found to have used or disclosed any information you have seen or heard whilst working within Burton and District Mind you may be dismissed from your volunteer role and possibly face legal action.

You must ensure that all records, including PC screens and computer printouts of registered data, are never left in such a manner that unauthorised persons can gain access to them. Paper records should always be locked away securely when not in use.

PC screens must always be locked when left unattended and you must ensure you log out of computer systems when finished. All computer passwords must be kept confidential to yourself.

I understand that I am bound by a duty of confidentiality and I agree to adhere to the conditions in the volunteering agreement with Burton and District Mind by which I am engaged and also to my personal responsibilities to comply with the requirements of the Data Protection Legislation.

I also agree to abide by the requirements set out within this document for the handling of Burton and District Mind's personal data.

Manager's Name: Job Title: .....

Signed ..... Dated .....

Appendix C:

Mind Burton and District

Third Party/Partner Risk Assessment and Checklist Procuring managers in Burton and District Mind are accountable for ensuring that mandatory requirements are applied and therefore take suitable precautions to safeguard its information.

Procuring managers engaging third parties on behalf of Burton and District Mind must ensure that they meet Information Governance standards and, where personal data is transferred or held, that an Information Governance risk assessment has been undertaken.

The following risk assessment should be carried out where personal data, including confidential beneficiary or donor information, is to be shared.

1 What is the purpose and objectives of the information sharing?

2 What Mind information assets or information processing facilities will the third party need to access?

3 What type of access will the third party have? – specify physical access and/or logical access, whether the access is taking place on-site or off-site and the exact location from which access will be made.

4 What is the value and classification of the information that will be accessed? (i.e. Confidential: client information, Confidential: commercially sensitive information, Protected internal information etc.).

5 Are there any information assets that the third party are not intended to access and which may require additional controls to secure?

6 Identify any of the third party's personnel, including their contractors and partners, who will or might be involved.

7 How will third party staff be authenticated?

8 How will the third party process, communicate and store the information?

9 What would be the impact to the third party of access to Burton and District Mind information assets not being available when required, or of inaccurate or misleading information being entered, received or shared?

10 How will Burton and District Mind's information security and/or incident management procedure need to be extended to incorporate information security incidents involving the third party?

11 What legal, regulatory or other contractual issues need to be taken into account with respect to the third party relationship?

12 What will happen to any shared information or assets on project closure? Attach supplementary sheets where necessary Append this risk assessment to the finalised contract Managers should check the following has been undertaken when establishing contracts with third party suppliers where personal data, including confidential beneficiary/donor information is to be shared:

13 No Check;

1 Carrying out the necessary vetting and information risk assessment of the third party before engagement.

2 Ensuring that all third party companies and individuals read and sign the relevant appendices of Mind's Confidentiality Agreement for Third Parties.

3 Ensuring that third party suppliers understand their responsibilities and to make available to them all guidance to enable them to meet Mind standards and requirements.

4 Ensuring that the third party is aware of personal data incident reporting requirements.

5 Ensuring that beneficiary, staff and business sensitive information is secure and not accessible to third party staff unless required for them to fulfil their contract.

6 Authorising the appropriate building/system access controls and where system access has been authorised, to inform the appropriate quarters when the contract finishes.

7 Ensuring that any equipment, material provided is returned to the procuring manager.

8 Ensuring that where contract staff work remotely that they are provided with appropriate mobile encrypted devices to ensure the security of data.

9 Ensuring the security arrangements of the third party and any subcontractors used are adequate.

10 Ensure that the Third Party Agreement is completed and signed and reviewed when any changes occur to the original contract.

Appendix D:

Confidentiality Agreement for Third Party Suppliers Introduction

This agreement is to be used as part of Burton and District Mind's work with third parties, partners or contractors to carrying out work on its behalf. Burton and District Mind as the 'Data Controller' under the Data Protection Bill 2018 has a legal responsibility for any Personally Information processed on its behalf by any third party or partner. Burton and District Mind could be in breach of the Data Protection Bill 2018 if it does not ensure that work conducted by others on its behalf meets the Information Governance standards. The Data Protection Bill 2018 draws a distinction between one data controller sharing personal data with another and a data controller sharing data with a 'data processor'. The Data Protection Bill requires the data controller using a data processor to ensure, in a written contract, that:

- the processor only acts on instructions from the data controller
- the processor has adequate security in place that is equivalent to that imposed on the data controller by the principles of the Data Protection Bill.

Third Parties Covered By this Agreement This agreement applies to all third parties and their sub-contractors when engaged by Mind in any capacity and for any period of time. Third parties will generally be defined within their specific contract, whether working on site or off site. They could include external agencies working under Service Level Agreements (SLA's), national or local contracts and include the following:

- Hardware and software maintenance and support staff
- Agencies or individuals processing data on behalf of Mind
- Agencies or individuals providing beneficiary services
- Consultancy and IT contract support staff
- Cleaning, catering, security guards and other outsourced support services (contracts should be signed by employing companies and by individual staff)
- Temporary agency staff
- Self-employed counsellors, counselling supervisors, or other service delivery staff

- Workforce placements Contractor undertaking The Contractor hereby undertakes:
- To treat as confidential all information which may be derived from, or be obtained, in the course of the contract, or which may come into the possession of the contractor, or an employee, servant or agent, or sub-contractor of the contractor, as a result, or in connection with the contract; and
- To provide all necessary precautions to ensure that all such information is treated as confidential by the contractor, his employees, servants, agents or subcontractors; and
- To ensure that he, his employees, servants, agents and sub-contractors are aware of the provisions of the Data Protection Act 1998 and that any personal data obtained from Mind shall not be disclosed or used in any unlawful manner; and
- To indemnify Mind against any loss arising under the Data Protection Bill 2018 caused by any action, authorised or unauthorised, taken by himself, his employees, servants, agents or sub-contractors. All employees, servants, agents and/or sub-contractors of the Contractor, will be required to agree to and sign an individual confidentiality agreement when they come to sites where they may see, or have access to confidential personal and/or business information or where confidential information is provided to them off-site.

Data Supplier Code of Practice –

The following Code of Practice applies where access is obtained to Burton and District Mind personal data, as defined within the Data Protection Bill 2018, for the purpose of preventative maintenance, fault diagnosis, hardware or software testing, repair, upgrade, replacement or any other related activity or data processing. The access referred to above may include:-

- Access to data/information on Burton and District Mind premises
- Access to data/information from a remote site
- Examination, testing and repair of media (e.g. fixed disc assemblies)
- Examination of software dumps
- Data processing using Dorset Mind information

The Supplier must certify that his organisation is registered appropriately under the Data Protection Bill 2018 and legally entitled to undertake the work proposed. The Supplier must undertake not to transfer the personal data outside of the European Economic Area (EEA). The Supplier must ensure that they, their employees and any sub contracted staff do not transfer, transmit or transport any

Burton and District Mind sourced or related electronic data / information to or via either their own laptops, computers, servers, USB memory sticks or any other media, portable or otherwise, unless the data is encrypted. The work shall be done only by authorised employees, or agents of the contractor (except as provided in paragraph below) who are aware of the requirements of the Data Protection Bill 2018 and of their personal responsibilities under the Data Protection Bill to maintain the security of Burton and District Mind's personal data. While the information is in the custody of the contractor it shall be kept in appropriately secure means. Any information sent from one place to another by or for the contractor shall be carried out be secure means. These places should be within the suppliers own organisation or an approved sub-contractor. Information which can identify any beneficiary/employee of Burton and District Mind must only be transferred electronically if previously agreed by Burton and District Mind and meets internal policies and procedures. This is essential to ensure compliance with strict regulatory controls surrounding the electronic transfer of identifiable personal data and hence compliance with the Data Protection Bill 2018. This will also apply to any direct-dial access to a computer held database by the supplier or their agent. The information must not be copied for any other purpose than that agreed by the supplier and Burton and District Mind. Where personal information is recorded in any intelligible form, it shall either be returned to Burton and District Mind on completion of the work or disposed of by secure means and a certificate of secure disposal shall be issued to Burton and District Mind. Where the contractor sub-contracts any work for the purposes above, the contractor shall require the sub-contractor to observe the standards set out in above. Burton and District Mind reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party. Burton and District Mind will expect an escalation process for problem resolving relating to any breaches of security and/or confidentiality of personal information by the suppliers employee and/or any agents and/or sub-contractors. Contract staff must report any observed or suspected security / confidentiality incident, including weaknesses identified in systems, design or operational procedures that are likely to give rise to an information security incident. This includes the potential disclosure of confidential personal information. Any information breaches or suspected information breaches made by the supplier's employees, agents or sub-contractors will immediately be reported to the individual in charge of GDPR compliance at Burton and District Mind and an Incident Report must be completed. Demonstration/loan systems with personally identifiable data in any form must have this data removed before equipment is removed from the premises. If this is not immediately possible then the supplier must secure the data to ensure that no unauthorised access is possible prior to deletion of the data. Any major lapse of this agreement will mean that the supplier may be held to be in breach of the contract and therefore subject to potential penalties.

Name of Contractor/Supplier (Print Name): .....

Address of Contractor/Supplier: .....

Telephone Number: .....

Email address: .....

On behalf of the Contractor/Supplier I certify that:

• I have read the terms of this agreement and agree to abide to the conditions set out. I understand my responsibilities for the security and confidentiality of personally identifiable information, under the Data Protection Bill 2018.
• The organisation is appropriately registered under the Data Protection Bill 2018 and is legally entitled to undertake the work agreed in the contract agreed with Burton and District Mind.
• In discharging the contract with Burton and District Mind the organisation will abide by the requirements set out within this document for the handling of Burton and District Mind's personal information which is either disclosed or otherwise accessible to my organisation during the period of the contract.

Name of Individual (Print Name): .....

Job Title: .....

Signature: .....Date: .....

On behalf of Burton and District Mind I certify that the necessary vetting and information risk assessment of the third party has been carried out before engagement. I have ensured that the third party is aware of Burton and District Mind's personal data incident reporting requirements and that all person identifiable data and business sensitive information is secure and not accessible to the third party staff unless required for them to fulfil their contract.

Approved by (Print Name): .....

Job Title at Mind: .....

Signature (on behalf of Mind)..... Date: .....

Responsibilities The Chief Officer is responsible for managing this policy and overseeing its implementation. The senior management team are responsible for implementing the policy within their areas of work, and for overseeing adherence by

staff and volunteers. Every member of staff should take personal responsibility for conforming to it.

Associated Policies and Procedures -

- Confidentiality Policy
- Data Protection and Security Policy
- Safe Haven Procedure
- Consent to Disclose
- Counselling Contract

Policy created 2021 - adopted by the board of trustees – Date .....