

Confidentiality Policy

Contents

1.	Introduction & Background	4
2.	Purpose.....	4
3.	Policy Statement.....	5
4.	Scope.....	5
5.	Definitions.....	5
	Confidentiality	6
	Data Protection	6
	Personal data	6
	Sensitive data.....	6
6.	Responsibilities	6
7.	Information to be Kept Confidential	7
8.	Maintaining Confidentiality	7
	8.1 General rules	7
	8.2 Handling confidential information	8
	8.3 Computers and confidentiality.....	8
9.	Collecting Personal Data	9
10.	Collecting Sensitive Personal Data	10
11.	Information Obtained by Clients.....	11
12.	Access to Confidential Information	11
13.	Sharing Information Outside the Organisation	11
	13.1 Consent to disclose	11
	13.2 Subject Access Requests	12
	13.3 Sharing information with third parties (i.e. services delivered in partnership) 12	
14.	Disclosure.....	13
	14.1 Disclosure and the “Duty of Care”	13
	14.2 Legal duty to disclose.....	13
	14.3 Consideration of when to disclose.....	14
15.	Managing an information breach.....	15
16.	Consequences for Deliberate Breaches	15
17.	Preserving Confidentiality in Other Processes	15
	17.1 When making a complaint.....	15

17.2	When writing to Nottinghamshire Mind	16
18.	Disposal	16
19.	Policy Implementation.....	16
20.	Monitoring and Review	17
21.	Version Control	17
22.	Related policies and Procedures	18
23.	Appendices	18
	Appendix 1 - Contract Confidentiality Clause – Staff.....	18
	Appendix 2 - Confidentiality Agreement – Volunteers and Placements.....	20
	Appendix 3 - Third-party Risk Assessment and Due Diligence Checklist	21
	Appendix 4 - Information (Personal Data) Breach Procedure.....	23

1. Introduction & Background

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

Nottinghamshire Mind aims to strike a balance between encouraging openness, avoiding unnecessary secrecy and bureaucracy, while ensuring individual privacy is respected. The confidentiality policy and associated procedures set the framework within which personal and any other potentially sensitive information is to be collected, stored, handled and disclosed.

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.

2. Purpose

The purpose of this policy is to explain how information should be handled and/or processed to maintain confidentiality, the circumstances in which confidentiality may be breached and the procedure for responding.

This policy aims to:

- Protect anyone involved with Nottinghamshire Mind from the possibility of information about them being passed on to individuals or organisations who have no right to that information.
- Reassure clients that good care will be taken with information which they give to Nottinghamshire Mind employees and volunteers and to be clear as to the circumstances when information can be shared with others.
- Provide guidance to employees and volunteers on the extent to which confidentiality is to be preserved, circumstances in which they may breach confidentiality, and measures to be taken for the safeguarding of information.
- Assist Nottinghamshire Mind employees and volunteers in complying with legal and statutory requirements for the disclosure of information.
- Reassure clients wishing to make a complaint to or about Nottinghamshire Mind, that the confidentiality of any complaint will be given high priority in so far as this is consistent with the need to investigate the complaint.

3. Policy Statement

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

When working with Nottinghamshire Mind you must:

- Treat all personal data and sensitive organisational information as confidential to Nottinghamshire Mind.
- Comply with the law regarding the protection and disclosure of information (including the UK GDPR and Data Protection Act 2018) and our policies, including our Information Governance and Data Protection Policy and any information sharing agreements

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

4. Scope

The policy and procedures in this policy (referred to as this Policy) are applicable to staff, volunteers, trustees, contracted third parties and members of consultative fora. If you are in any doubt about the application of this Policy, please seek guidance from a manager or the individual in charge of GDPR compliance.

This Policy is designed to work alongside, and support, guidance used by Nottinghamshire Mind on safeguarding children and young people, safeguarding adults, data protection, privacy and use of information technology. It should be read in conjunction with the Information Governance and Data Protection Policy, Privacy Policy and staff should be made aware of the information sharing agreements specific to their service area.

This policy applies to:

- Personal and sensitive data from all sources – including staff, volunteers, clients, trustees.
- Sensitive organisational data – e.g. unpublished financial information, intellectual property, tenders and bid applications.
- Anyone at Nottinghamshire Mind who has access to confidential information/data.

5. Definitions

It is perhaps helpful to explain the difference between confidentiality and data protection; and between personal and sensitive data.

Confidentiality is about privacy and respecting someone's wishes. There is an expectation that information will not be shared.

It:

- Relates to all forms of information about people using services, employees and volunteers – no matter how it was obtained.
- Also applies to information about the organisation – particularly anything that could be business sensitive.
- Doesn't matter if this information has been formally recorded or not.

Data Protection is concerned with how we collect, process, use and store someone's information.

It:

- Concerns personally identifiable information relating to a *living individual* and which is recorded and stored in a retrievable system – no matter in what format.

Nottinghamshire Mind's duties and obligations with regards to data protection are set out in our Information Governance and Data Protection Policy, which is supported by our Privacy Policy.

Personal data is information that relates to a living individual. That individual must be identified or identifiable either directly or indirectly from one or more identifiers or from factors specific to the individual. Such identifiers include data such as name, address, NHS number, location data, online identifier.

Sensitive data (also known as Special Category data) is data that is likely to be more sensitive and is therefore given extra protection under the Data Legislation. Such data relates to an individual's racial or ethnic origin; political opinions; philosophical or religious beliefs; trade union membership; genetic data; biometric data (where used for identification purposes); health; sex life; or sexual orientation.

6. Responsibilities

All Nottinghamshire Mind employees and volunteers are required to respect the right of clients and of other employees and volunteers to privacy and confidentiality as far as possible within the constraints of legal requirements and the safety of other people. Absolute confidentiality cannot be guaranteed. It will be made clear to clients at the earliest possible opportunity the circumstance in which this could happen (e.g. as part of the counselling agreement).

Any sharing of confidential information, outside of that contained in the service information sharing agreements, must in the first instance be checked and approved by the relevant service lead, or if not available the Operations Manager or CEO.

Where the need to share information is in relation to a safeguarding issue, the Safeguarding Officer is delegated to approve the breach on the CEO's behalf. In these circumstances, Nottinghamshire Mind's safeguarding procedures must be adhered to throughout. Please see our Safeguarding policies for more information.

7. Information to be Kept Confidential

All personal data and confidential information about Nottinghamshire 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.

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 damage Nottinghamshire Mind's reputation or business operations.

8. Maintaining Confidentiality

All personal data should be treated in the strictest confidence and in accordance with our Information Governance and Data Protection Policy. Personal data should only be disclosed outside Nottinghamshire Mind in line with our Privacy Policy and relevant information sharing agreements. If you are uncertain as to whether data can be shared, do not share it; seek clarification from your line manager or the Data Protection Officer.

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 their manager.

8.1 General rules

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

- Do not share confidential information with those who have no right, or do not need, to see or know it.
- Take steps to avoid being overheard when discussing confidential information, particularly in areas open to the public or in communal and open plan areas.

- Get into the habit of checking and clearing your work area at the end of the day.
- Keep records which include no more than the minimum information required to provide the required service and/or support.
- Never leave confidential information unattended, lock it away when not in use.
- If you need to take sensitive documents away from the office, seek permission first.
- If you do have to take confidential documents away from the office you must store them securely and not show them to others.
- Do not read or process confidential documents on public transport.
- Do not leave confidential information unattended in cars or public places.
- Destroy information when it is no longer required, by shredding or confidential waste disposal (see our Record Retention procedure for guidance on this if required).
- Remember that information in the wrong hands can cause a lot of damage and unnecessary stress.
- Simply put, we should treat other people's personal information in the same way we would want ours to be treated.

8.2 Handling confidential information

Care should be taken at all times when handling confidential information. For example:

- In meetings, you should only disclose information that is relevant to the discussion/decision.
- When writing to an individual, you should check that you can write to them at their home address or make arrangements for letters to be sent elsewhere.
- When emailing an individual, extra care should be taken to ensure the correct email address is being used.
- When printing or copying documents containing personal information, ensure that you collect the printing quickly and do not leave documents sitting in or on the printer.

8.3 Computers and confidentiality

Computers and other digital devices are essential in carrying out our day-to-day work. However, we must always be mindful to ensure that high levels of data security and confidentiality are maintained. Staff should familiarise themselves with, and follow the guidance in, our Acceptable Use of Information and Communication Technology policy.

In addition:

- When not in use, computers should be locked or users should log out to prevent unauthorised access.

- All user accounts must be protected by strong passwords and passwords to be held securely by the owner. Passwords must be changed regularly in accordance with our Acceptable Use of Information and Communication Technology policy.
- No disks, CDs or other portable storage media should be used to store personal data of any kind.
- No Nottinghamshire Mind data or documents should be saved on the hard drive of any computer, laptop, tablet or other device.
- Staff should be aware that when accessing documents on Charity Log, these will automatically download to their device; staff should ensure that they permanently delete the file when no longer required and to also periodically clear the download history on their device.
- Everything must be saved to SharePoint, the Microsoft Cloud storage used by Nottinghamshire Mind. There could be random checks to ensure this policy is being adhered to.
- Unless it is absolutely necessary and the data cannot be shared by other means, no personal data should be transferred via email; if there is an occasion where this is required the data should either be encrypted or password protected.
- The Bcc facility on e-mail should not be used as a mechanism for sharing or distributing personal data of any kind.
- The Bcc facility should always be used when sending an email to a group distribution where that group includes individuals who are not employees at Nottinghamshire Mind (ie individuals who do not have an @nottinghamshiremind email address).
- When staff or volunteers leave the organisation, all electronic and digital devices must be returned to Nottinghamshire Mind where the data will be deleted and the device returned to its original factory settings.

9. Collecting Personal Data

You should ensure that all personal data you collect and 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 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.

Wherever possible, when collecting 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. Consent can be either verbal or written, and must be recorded on the individual's personal record. (Please see below, if collecting sensitive personal data such as health information). 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 policy or refer them to the privacy notice on [Nottinghamshire Mind's website](#) for more information.

Nottinghamshire Mind's referral processes are the primary source of personal data for the individuals that we work with. All referral forms include statements to demonstrate consent (by an affirmative action) that:

- Nottinghamshire Mind can store, use and process the information provided for the purposes outlined.
- The personal and health information provided can be shared with Nottinghamshire Mind.

10. Collecting Sensitive Personal Data

There is a greater weight of responsibility, and therefore protection, where sensitive personal data (or special category data) is concerned. This is because use of this data could create significant risks to the individual's fundamental rights and freedoms.

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:
 - The purpose of recording the data and how it will be used.
 - Who will have access to it and whether it will be shared with third parties.
 - 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.

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 Nottinghamshire Mind to undertake a particular activity for a given individual.

11. Information Obtained by Clients

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

Clients involved in group work/peer 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.

Nottinghamshire Mind will make clients aware of their responsibilities under these circumstances and they are responsible for ensuring they comply.

12. Access to Confidential Information

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

All employed staff, sessional workers and volunteers must sign a confidentiality agreement before being given access to Nottinghamshire Mind information assets. For paid staff this agreement forms part of their contract of employment (See [Appendix 1](#)). For volunteers (including placements and trainees) it is covered by Nottinghamshire Mind's volunteer confidentiality agreement (See [Appendix 2](#)).

See [Section 13.3](#) for information about we manage third-party agencies and contractors who require access to confidential information.

13. Sharing Information Outside the Organisation

Where it is thought necessary to pass on information to another individual or organisation this will be assessed on the basis of their application and full consideration of whether there is a legal duty to disclose information.

13.1 Consent to disclose

The individual concerned (eg client, volunteer, staff member) will be advised, preferably in writing, that information has been requested and by whom. Where possible, the consent of the person about whom the request has been made will be sought.

Consent will be recorded in the individual's record (eg Charity Log, personnel record) with the date consent was obtained, whether it was written, electronic or verbal and brief details of the request to disclose.

Where the individual concerned strongly objects to information being passed to a third-party, they should be advised that they should seek legal advice.

The process of informing the person and seeking consent need not be followed where the consent of the person concerned can be implied, for example where a reference is requested, where the Dept. of Employment asks for information about a former employee in order to pay benefit or when a service user has signed a disclaimer on a referral form.

13.2 Subject Access Requests

Clients have a right to see their personal files and the data we hold on them. Requests from individuals to access their own data will be managed in accordance with our Subject Access Request Process as outlined in our Information Governance and Data Protection Policy. We ask that any such requests are made in writing.

The individual does not have to specify that they want to make a request under Data Protection Legislation, or to use the words ‘Subject Access Request’. If we reasonably consider that is what they are asking for - we must act on it accordingly. Subject Access Requests must be responded to within one month of receipt.

Requests from anyone seeking access to their records, should be sent to the Data Protection Officer - dataprotection@nottinghamshiremind.org.uk

13.3 Sharing information with third parties (i.e. services delivered in partnership)

External agents and contractors who process personal data and other confidential information on behalf of Nottinghamshire Mind must be made aware of Nottinghamshire 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 Nottinghamshire Mind’s information assets.

All agents and contractors in receipt of Nottinghamshire Mind confidential information should complete and sign a confidentiality agreement at the outset of the contract being established.

Where those third parties are specifically processing personal data (as a data processor) for Nottinghamshire Mind, the contract should also set out that Nottinghamshire Mind is the data controller and the third-party is a data processor and the respective obligations of both parties under the Data Protection Legislation.

Nottinghamshire Mind managers responsible for contracting with third-party organisations where access to Nottinghamshire 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 3](#). They should also ensure that any individual whose data may be subject to being shared with a third-party is made aware of this fact through a privacy notice, and this fact recorded accordingly.

14. Disclosure

Disclosure of personal data and other confidential information should only be made in accordance with Nottinghamshire Mind's Information Governance and Data Protection Policy, Privacy Policy and any information sharing agreements.

14.1 Disclosure and the “Duty of Care”

Nottinghamshire Mind owes a "duty of care" to the users of its services and to its staff. It may therefore be necessary to breach confidentiality where a client is acting, or likely to act, in a way that could cause serious harm to him or herself or put other service users or staff at risk.

Nottinghamshire Mind also owes a general duty of care towards members of the public. It may be necessary to pass on information to the police or statutory authorities where there is considered to be a serious risk to a particular person or persons, or to the public in general.

Nottinghamshire Mind employees and volunteers share with all citizens a duty of care towards children and vulnerable adults. Staff should always act in accordance with Nottinghamshire Mind’s Safeguarding Policies when making safeguarding reports.

- If Nottinghamshire Mind workers know or suspect that **a child** is at risk of harm or neglect the [Safeguarding children - Multi-Agency Safeguarding Hub \(MASH\)](#) must be informed.
- If Nottinghamshire Mind workers know or suspect that a vulnerable **adult** is at risk or abuse or neglect, the [Safeguarding adults - Multi-Agency Safeguarding Hub \(MASH\)](#) must be informed

14.2 Legal duty to disclose

The law in general does not give an absolute right to confidentiality except where there is a contractual provision to this effect.

Legal and statutory requirements affecting Nottinghamshire Mind include, but are not limited to:

- Reporting notifiable occupational diseases to the [Health and Safety Executive](#) where appropriate (see our Health & Safety Policy for information)
- Reporting accidents at work, in certain circumstances, to the [Health and Safety Executive](#) (see our Health & Safety Policy for information)

- Replying to certain specific enquiries from Government Departments E.g. Dept. of Employment or Dept. of Social Security, or the Inland Revenue. Not all such enquiries are covered by statutory requirements so a check on the legal status of the request should be made before supplying information.
- Providing names of residents of a house in multiple occupation for Council Tax purposes, if Nottinghamshire Mind is designated the "responsible person".
- Passing on information on terrorist activities and information requested on road accidents involving personal injury, to the police.
- Reporting on trafficking of humans or illegal substances that comes to the notice of Nottinghamshire Mind staff or volunteers.
- Giving evidence in court if a subpoena is issued.

There is no absolute duty to provide the Police with information except in the case of **suspected or actual terrorism**. However, Nottinghamshire Mind's policy is that its employees and volunteers have a duty in the public interest not to withhold from the police any information concerning criminal activity of a serious nature. This should preferably be done with the knowledge of the person concerned and whenever possible with their cooperation but there may be circumstances where the risk to others is too great for this to be advisable or possible.

14.3 Consideration of when to disclose

Where there is a legal duty to pass information to others, such information will only be passed after discussion and approval by the CEO. Staff are not permitted to pass on such information.

Where there is no legal obligation but there may be a duty of care to pass on information the decision whether or not to do so will in the end remain one of individual judgement.

Points for consideration are:

- Is the risk a real one?
- How great is the danger to self or to another person?
- Will the breach of confidentiality avoid the harm?
- Is there no other way of avoiding the harm?

Where it is decided that information must be passed on to another individual or organisation the basis on which disclosure is to be made must be clear and unambiguous. Those disclosing the information must first have an understanding as to the intended use of the information requested and by whom.

Requests from statutory bodies must be submitted in writing, even when there is a legal obligation on Nottinghamshire Mind to comply with the request.

15. Managing an information breach

If an information breach occurs, the responsible Nottinghamshire 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.

The breach must be reported to the Data Protection Officer, in line with our Information Breach Procedure as detailed in [Appendix 4](#).

Where a complaint is received in relation to an information breach, this will be managed through our complaints process in accordance with our Comments, Compliments and Complaints Policy.

It does not matter if the breach concerns data that is held electronically or is in relation to paper records. If the information that has been disclosed is personal, sensitive or business sensitive then Nottinghamshire Mind considers this to be a data breach.

16. Consequences for Deliberate Breaches

The effects of a deliberate breach of confidentiality that does not follow policy are far-reaching, and include:

- Damage to organisational reputation
- Loss of trust from funders, donors, clients, public etc
- Financial implications
- Disciplinary procedures

Staff should be made aware of, and follow guidance within, the Whistle-Blowing Policy with regards to the circumstances and processes around information sharing outside of formal data disclosures.

17. Preserving Confidentiality in Other Processes

17.1 When making a complaint

People who wish to make a complaint either to Nottinghamshire Mind about another agency or individual or about an aspect of Nottinghamshire Mind's services, employees or volunteers may be concerned about the confidentiality of information they are giving. The preservation of confidentiality will be given high priority, subject to the exceptions listed above/or if it is necessary to breach confidentiality in order to properly investigate the complaint. The permission of the complainant will always be sought for this but in

cases where the welfare of the complainant or other people is seriously at risk it may be necessary to breach confidentiality even if that permission is withheld.

17.2 When writing to Nottinghamshire Mind

When a letter about an individual is written to Nottinghamshire Mind by a professional or carer the writer should be informed that the client is permitted access to his/her file and their advice sought on what action they wish Nottinghamshire Mind to take. This could include returning the letter to the sender or, in exceptional cases, keeping the letter in a separate confidential place.

18. Disposal

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

All data and information held by Nottinghamshire Mind will be stored in line with our Information Governance and Data Protection Policy and Records Retention procedure. All records, be they physical or electronic/digital will be archived, in accordance with the Records Retention procedure, in a secure setting until the end of the relevant retention period, at which time they will be securely destroyed.

19. Policy Implementation

The CEO and the Board of Trustees is responsible for gaining assurance that confidentiality is managed appropriately within Nottinghamshire Mind and that adequate resources are made available to implement this Policy.

The CEO 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.

The HR Manager is responsible for ensuring that confidentiality clauses are contained within all contracts and that confidentiality training is included in all inductions.

The Volunteer & Placement Lead is responsible for ensuring that all volunteers, trainees and placements understand and sign the confidentiality agreement and that confidentiality training is included in all inductions.

Line Managers will be responsible for ensuring that all Nottinghamshire Mind staff working in service delivery role have read this Policy, any relevant information sharing agreements 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 training for staff.

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

20. Monitoring and Review

The implementation of this policy will be monitored through an annual review of complaints and comments received, specifically where sharing of information is part of the concern.

This policy will be reviewed every three years, or when legislation or other statutory guidance impacting on it changes.

Staff, volunteers and trustees will be made aware of the changes to the policy through all means available (eg SharePoint, Breathe, Intranet).

21. Version Control

Version Number	Purpose/Change	Owner/Author	Date	Review
1.0	Created by Nic Roberts	Nic Roberts, CEO	01/04/2018	01/04/2021
1.1	Reviewed and updated with new content to bring into line with MQM checklist and Data Protection and Privacy policies; Appendices added	Katie Freeman, Project Support	28/10/2022	Nov 2025

Date adopted by Trustees	17/11/2022	Date Published	03/01/2023	Date for Next Review	Nov 2025
Approved by	Derek Adlam, Trustee Christina Bond, Trustee Roger Stendall, Chair				

22. Related policies and Procedures

- Access to Information
- Code of Conduct
- Compliments, comments and complaints
- Information Governance and Data Protection
- DBS Checking procedure
- Managing positive DBS disclosures
- Disciplinary
- Financial procedures
- Home-working
- Privacy Policy
- Records Retention procedure
- Safeguarding – both Adults and Children & Young People
- Trustee recruitment and induction
- Use of IT and IT Security
- Use of Social Media Policy
- Volunteering
- Whistle-Blowing Policy

23. Appendices

Appendix 1 - Contract Confidentiality Clause – Staff

Appendix 2 - Confidentiality Agreement – Volunteers and Placements

Appendix 3 - Third-party Risk Assessment and Due Diligence Checklist

Appendix 4 - Information (Personal Data) Breach Procedure

Appendix 1 - Contract Confidentiality Clause – Staff

Confidentiality

Employees are expected to treat all personal and sensitive information received in the course of their duties in a discreet and sensitive manner, observing confidentiality at all times.

Employees shall take all reasonable care to keep safe all materials containing confidential information, and shall at the time of termination with us, or at any other time, return any such material in their possession.

See employer’s confidentiality policy for full details.

Staff are prohibited from talking to press without prior consent from the CEO.

Appendix 2 - Confidentiality Agreement – Volunteers and Placements

All volunteers, trainees and student placements who join Nottinghamshire Mind, are required to sign a [Confidentiality Agreement](#) as part of their onboarding process. When signed a copy will be uploaded to their volunteer record on Charity Log.

A copy of this is located in SharePoint > Volunteering > Volunteer Process

The confidentiality agreement outlines volunteer responsibilities with respect to:

Working with data

- Describes what constitutes personal information and sensitive personal information.
- Highlights the “Do’s and don’ts” of maintaining confidentiality.

Confidentiality expectations

- Duty of confidentiality is not restricted to personal data.
- We have a duty of care to the people who use our services and volunteers should be aware that there could be situations where it might be necessary to breach confidentiality.
- Volunteers should not under any circumstance share confidential data; they should always contact their supervisor so that action can be taken if necessary.
- Simply put, we should treat other people’s personal information in the same way we would want ours to be treated.

Appendix 3 - Third-party Risk Assessment and Due Diligence Checklist

Procuring managers in Nottinghamshire 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 Nottinghamshire Mind must ensure that they meet Information Governance standards.

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

No		Check
1	What is the purpose and objectives of the information sharing?	
2	What Nottinghamshire 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 Nottinghamshire Mind information assets not being available when required, or of inaccurate or misleading information being entered, received or shared?	
10	How will Nottinghamshire 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 additional sheets where necessary to demonstrate discussion and decisions taken		
Append this risk assessment to the finalised contract.		

<i>Service/Project (or name of individual)</i>			
<i>Name of person completing checklist</i>		<i>Date</i>	
<i>Role</i>			

Third-Party Due Diligence Check

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:

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 breach 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 responsible leads when the contract finishes.	
7	Ensuring that any equipment or 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 sub-contractors used are adequate, including a review of their data protection arrangements where deemed appropriate and necessary.	
10	Ensure that an appropriate information sharing agreement is completed, signed and appended to the contract, and that it is reviewed when any changes occur to the original contract.	
When completed this checklist should be appended to the final contract.		

<i>Service/Project (or name of individual)</i>			
<i>Name of person completing checklist</i>		<i>Date</i>	
<i>Role</i>			

Appendix 4 - Information (Personal Data) Breach Procedure

What do we mean by an information (personal data) breach?

An information breach is when personal or sensitive data belonging to an individual, or a group of individuals, is disclosed to a third-party without the individual's consent.

The information may have been disclosed by a member of staff or volunteer or obtained through loss or theft of either equipment or data.

All personal data breaches should be reported to the Data Protection Officer – dataprotection@nottinghamshiremind.org.uk – immediately that you become aware of them. We have a duty to respond urgently to all breaches of personal data.

Responding to a personal data breach

If we think there's been a personal data breach – perhaps an email has been sent to the wrong person, a laptop was stolen from a car or you've lost files because of a flood – and you're worried about what to do next, we should take the following steps:

Step one: Don't panic

1. Inform the Data Protection Officer (DPO) immediately – they will lead the investigation and response.
2. Tell the DPO everything that you know about the incident – how you became aware of it, what you believe happened and any impact that you are aware of
3. The DPO will open a breach log to record what happened and what steps are taken to respond. The log includes:
 - the causes of the personal data breach
 - what happened
 - the personal data affected
 - the impact on those affected
 - any steps the business took to reduce the consequences to those affected
 - the reasons for deciding whether or not to report it to the ICO

Not every breach reported to the ICO results in formal action. The main aim of the ICO is to provide advice to help organisations avoid similar incidents in the future.

Step two: Start the timer

4. The DPO will urgently liaise with members of the Management Team to consider whether we need to report the breach to the ICO; the DPO will use the ICO's [self assessment tool](#) to support this decision making.

By law, we have to report a [personal data breach to the ICO](#) without undue delay (if it meets the threshold for reporting) and within 72 hours. The clock starts from when we discovered the breach, not when it actually happened.

When deciding whether we should report a breach to the ICO, we must consider:

- the severity of the impact on the rights and freedoms of the affected individuals;
- the scale of the data breach (ie how many people are affected);
- the extent of any interference with the right to privacy under Article 8 of the European Convention on Human Rights (ECHR);
- whether the breach involves any personal data whose processing constitutes “sensitive processing”; and
- the nature of the rights and freedoms which have been impacted (eg a breach leading to a risk to the right to life under Article 2 ECHR would be particularly serious).

We might end up not needing to report the breach, but we should start a breach log anyway, to record what happened, who is involved and what we’re doing about it.

Step three: Find out what’s happened

5. The DPO will investigate what happened, liaising with staff members and Service Leads as necessary, to pull the facts together as quickly as possible.
6. The investigation should include things like what happened and why, how many people were involved, a timeline of when it all happened, and what actions have been taken so far.

Step four: Try to contain the breach

7. Our priority is to establish what has happened to the personal data affected. If we can recover the data, we must do so immediately. We should also do whatever we can to protect those who will be most impacted. For example:
 - If the data has been sent to someone by mistake, we will ask them to delete it, send it back securely, or (for paper records) have it ready for us to collect.
 - If we don’t know where it is, we should retrace what happened. For example if we think it’s been lost in an office or building, we could try calling the reception.
 - In the event of loss of IT or communications equipment the DPO will inform our IT Support Service (SME) immediately for advice and support, and request that the equipment be remotely wiped to minimise the risk of personal data falling into the wrong hands.
 - In the event of a cyber attack the DPO will inform our IT Support Service (SME) immediately for advice and support, and instruct all staff members to immediately change passwords on all devices and programs.

Step five: Assess the risk

8. We will assess what we think the risk of harm is to those affected, whether that's clients, volunteers, donors, members or employees.

Risk of harm: means any potential harm or detriment it may cause to people, eg safeguarding issues, identity theft or significant distress. For example, the breach might be the result of a simple mix-up where there's little or no risk involved, or a serious breach that will have a lasting effect on people's lives.

9. When assessing risk, it can help to put yourself into the shoes of those who have been impacted.

For example, supposing you email a hair appointment reminder to the wrong customer and they have deleted the email. If you were the customer you meant to remind, would you be worried? Unless there's more to this than meets the eye, it's unlikely you would need to tell the customer or the ICO.

The ICO's [guide](#) for small organisations on understanding risk in personal data breaches is a useful source of information and includes examples of different types of breaches.

Step six: If necessary, act to protect those affected

10. If possible, we should give specific and clear advice to people on the steps they can take to protect themselves, and what we are able to do to help them.

Depending on the circumstances, this may include advising people to use strong, unique passwords, telling them to look out for phishing emails or fraudulent activity on their accounts and providing guidance on protecting themselves from identity theft.

11. If we don't think there's a high risk to the people involved, we don't have to let them know about the incident.
12. We may decide to tell the people affected about the breach, even if we don't think there's a high risk to them. But we must balance any risk to them against the potential of causing unnecessary worry.
13. If we think there's a high risk, then by law we have to tell them without undue delay. For example, if we feel there is a high risk of them having their identity stolen, then we have to let them know so they can be extra vigilant and take steps to protect themselves.

Step seven: Submit your report (if needed)

14. If the breach is reportable we must report it to the ICO
 - Monday to Friday, 9am to 5pm – telephone 0303 123 1113
 - Evenings and Weekends – online [ICO|Report a breach](#)

15. We must provide details such as what happened and when, the risk assessment we have carried out, and what we've done to contain the breach.
16. It is OK if we don't have all the information to hand straight away – the important part is letting the ICO know that it's happened before 72 hours have passed. We can then provide more details later as part of a follow-up report if necessary. This should be completed without undue delay and we will treat it as an urgent priority.

Further information and support:

[Understanding and assessing risk in personal data breaches](#)

[Get help and support from the ICO](#)

Note: this information breach procedure is also contained in the appendices of the Information Governance and Data Protection Policy; ensure any changes are reflected in both.

END