Information Governance Policy

Reference:	*Information Governance Policy*
Date Originally Approved:	*April 2013*
Approving Body:	*Board of Trustees (delegated authority to Directors Team)*
Implementation Date:	*February 2021*
Version:	*1.0 (**VERSION 10.0 PRIOR TO UPLOAD TO 4POLICIES**)*
Supersedes:	
Stakeholder groups consulted:	*Information Governance Steering Group, Directors Team, Governance Committee*
Target Audience:	*Staff, Volunteers*
Review Date:	*February 2024 (or earlier if changes in law)*
Lead Executive	*Senior Information Risk Officer*
Author/Lead Manager:	*Head of Data & Insight*

Policy history

Version	Author	Date	Change
7.0	Elice Craske	03/05/17	Version 6.0 : Update to section 2.4 (Policies and procedures used by the Association):
			Removed reference to: Business continuity plans and procedures; Working at Home or Away from the Office Policy (re-titled); Commercial and Contractual Compliance Policy (does not exist); Management of Intellectual Property Policy (does not exist); Volunteer agreement (re-titled); Information incidents: guidelines on identifying and reporting information incidents (does not exist); Breach of data management procedure (does not exist as a procedure)
			Added: ICT recovery plan; Working at Home Policy; Mutual Expectations (Volunteers); Retention of Information Guidance; Data Protection Breach Tracking Form; IP Guidance
8.0	Karen Pearce	31/05/17	Version 7.0: Update following external assessment by Protecture as follows:
			Removed appendices: reference to policies, procedures and guidance replaced by hyperlinks to remove repetition across documentation
			Updated: simplification and clarification of wording. Reference to Data Protection Officer removed and replaced with Senior Information Risk Officer

Version	Author	Date	Change
9.0	Elice Craske	31/01/18	Version 8.0 updated by the Information Governance Steering Group, as follows:
			Lead Executive: Changed to Senior Information Risk Officer
			Author/Lead Manager: Head of Data & Insight
			Updated: reference to statutory and mandatory requirements changed to 'laws and regulations'.
			Updated: reference to personal data changed to 'personal information'
			Updated: Information Governance training changed to 'relevant information governance training'
			Removed: hyperlinks to all of the individual policies, procedures and guidance. **Added:** one hyperlink to the file save location for all information governance and data protection policies and procedures **and** one hyperlink to condition of employment policies
			Changed: Retention, Archiving and Destruction of information guidance **to** Retention, Archiving and Destruction of Information schedule
			Added: overall responsibility of the Senior Information Risk Officer (SIRO) is to ensure compliance with legislative and regulatory requirements
			Removed reference to: freedom of information responsibilities
			Removed reference to: design and review of performance indicators to measure compliance and progress against the Association's risk register
			Added: reference to the Data Protection Breach Reporting procedure within 2.6 (all staff and volunteers)
			Updated: Appendix A – Terms of Reference of the Information Governance Steering Group
	Elice Craske	24/04/18	**General formatting throughout document**
			Removed from 2.1: It plays a key part in clinical governance, service planning and performance management. (This is duplicated in section 1).
			Added within 2.5: All staff, whether permanent, temporary or contracted, and volunteers are responsible for making sure that they are aware of and comply with the requirements of this policy and the policies, procedures and guidance produced to support it. Where in doubt, support should be sought by a line manager, **the data team** or the SIRO.
			Added within 2.6 (all staff and volunteers): For our volunteers, the relevant policies are on the Volunteer Zone.
			Added within 2.6 (all managers): All managers are responsible for ensuring that all staff **and volunteers** are made aware of and comply with the policies, procedures and guidance which support Information Governance.

Version	Author	Date	Change
			Changed within 2.6: The Chief Executive is the Accountable Officer with overall responsibility for Data Protection and Information Governance within the Association and is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.
			Changed within 2.6: The Information Governance Steering Group informs and shapes the governance of information across the Association.
			Removed 2.7 (Approval)
10.0	Elice Craske	14/01/21	Version 9.0 updated as follows
			Terms of Reference updated
			Removed reference to Information Sharing Agreement within 2.4 – the ISA is not a specific policy, procedure or guidance.
			Updated the titles of policy names: Safeguarding Vulnerable Adults Policy changed to Safeguarding Adults at Risk of Harm Policy Working at Home Policy changed to Homeworking Policy Mutual Expectations (Volunteers) changed to Volunteering Policy

Information Governance Policy

Contents

1. Policy Statement of Intent

Information is a vital asset to the MND Association ('the Association'). It is used on a daily basis for the management of all of our work. As we deliver care and support, we have a responsibility to people with MND, staff, contractors, volunteers and all other supporters for the efficient management of services and resources. Information plays a key part in clinical/research governance, financial management, service planning, measuring and evidencing performance. Furthermore, the Association has a legal obligation to ensure that personal and sensitive information is managed appropriately.

It is of paramount importance to ensure that information is properly managed. It must be accurate, up-to-date, available at the point of need and appropriately retained and retrievable for future use. Staff and volunteers must understand their responsibility for information and receive/undertake relevant learning. This activity is supported by a series of policies and procedures, with management accountability and structures in place to provide a robust governance framework for information management both now and in the future.

Information Governance brings together the laws and regulations that apply to the handling of information, allowing:

- Giving of advice and guidance.
- Compliance with the law.
- Self-assessment audits and assurance processes to measure and report performance.
- Year-on-year improvement plans.
- Public confidence in the Association's management of personal information.
- Protection and maintenance of intellectual property.
- Commercial and contractual compliance.

This Information Governance Policy sets out the Association's approach to the governance of information in accordance with laws and regulations.

The policy will be reviewed and revised as and when it becomes necessary and at least every three years.

2. The MND Association's Information Governance Policy

2.1 Introduction

Information is a vital asset in terms of supporting service users, engagement with supporters and stakeholders and the efficient management of services and resources. It is, therefore, of paramount importance that information is safely, securely and effectively managed, and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for managing information.

2.2 Purpose of the policy

This Information Governance Policy provides an overview of our approach to information governance, a guide to the policies and procedures in use and details about the management structures that underpin the approach within the organisation.

2.3 The Association's approach to Information Governance

The Association strives to effectively govern our use of information, and will ensure the following:

- Information will be protected against unauthorised access and use.
- Information is managed confidentially.
- Information will be maintained accurately.
- Information will be supported by the highest quality data.
- Regulatory requirements will be met.
- Relevant information governance learning will be given to all staff and volunteers as necessary to their role.
- All actual or suspected breaches of confidentiality and information security by staff, volunteers or third parties and including both electronic and paper-based data, will be logged and reported immediately to the line manager and investigated.

2.4 Policies, procedures and guidance used by the Association

Information Governance will be managed through staff, volunteers and contractors abiding by the following policies, procedures and guidance:

- Data Protection policy and procedures:
  - Data Protection Policy
  - Data Protection Breach Reporting Procedure
  - Subject Access Request procedure
  - Sharing personal information guidance
- Condition of employment policies including:
  - Confidentiality Policy
  - Safeguarding Adults at Risk of Harm Policy
  - Safeguarding Children and Young People Policy
  - ICT User and Security Policy

- Homeworking Policy
- Website policies
- Privacy policy
- Photography policy
- Retention, Archiving and Destruction of Information schedule
- Intellectual Property Guidance
- Business continuity plans and procedures
- The Minimum Data Set (MDS) and Enhanced MDS guidance
- Voicemail and Call-back protocol
- Volunteering Policy
- Recruitment procedure
- Starters' procedure
- Leavers' procedure

2.5 Responsibilities and accountabilities

The designated Information Governance / Data Protection lead for the Association is the Senior Information Risk Officer (SIRO), with delegated authority from the Chief Executive. The key responsibility of the SIRO is to ensure compliance with legal and regulatory requirements including:

- Development and implementation of information governance policies, procedures and guidance.
- Raising awareness and providing advice and guidance to all staff and relevant volunteers.
- Ensuring learning needs are identified, developed and delivered.
- Co-ordinating the activities of all staff and volunteers relating to data protection, confidentiality, information quality and records management through the Information Governance Steering Group.
- Ensuring that data is kept secure and that all data flows, both internal and external, are regularly checked against any *Information Sharing Agreements* in place.
- Overview and assurance of information handling in the Association to ensure compliance with laws and regulations.
- Individuals whose data we retain and use are appropriately informed about the organisation's information handling activities.

The day-to-day responsibilities for providing guidance to staff, volunteers and contractors will be undertaken by relevant line managers.

The Association's Board of Trustees and the Chief Executive are responsible for ensuring that sufficient resources are provided to support effective Information Governance and ensure compliance with the law.

All staff, whether permanent, temporary or contracted, and volunteers are responsible for making sure that they are aware of and comply with the requirements of this policy and the policies, procedures and guidance produced to support it. Where in doubt, support should be sought by a line manager, the data team or the SIRO.

2.6 Information Governance structure and responsibilities

The Board of Trustees, via the Governance Committee, is ultimately responsible for information governance within the Association.

The Chief Executive is the Accountable Officer with overall responsibility for data protection and information governance within the Association and is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

The Senior Information Risk Officer (SIRO) will be a member of the Directors' Team and has responsibility delegated from the Chief Executive for ensuring that effective systems and processes are in place to deliver the data protection and information governance work. The SIRO chairs the Information Governance Steering Group and reports annually to the Governance Committee.

The Directors are accountable to the Chief Executive for ensuring the effective implementation of the underpinning policies and procedures for information governance within their respective directorates.

All Managers are responsible for ensuring that all staff and volunteers are made aware of and comply with the policies, procedures and guidance which support information governance.

All Staff and volunteers, whether permanent, temporary or contracted, including agency staff and contractors are responsible for ensuring they are aware of the information governance requirements and for ensuring they comply with these on a day-to-day basis. For ease, the key policies are the *Data Protection Policy*, the *Confidentiality Policy*, the *ICT User & Security Policy* and this *Information Governance Policy*. For our volunteers, the relevant policies are on the Volunteer Zone. Any identified breach of information management will be reported by staff or volunteers immediately to their respective line managers. The *Data Protection Breach Reporting Procedure* must then be followed.

The Information Governance Steering Group informs and shapes the governance of information across the Association (Appendix A: Terms of Reference Information Governance Steering Group). The Steering Group will ensure the development and maintenance of policies, procedures and guidance and the development of an information governance framework. The SIRO chairs the Information Governance Steering Group and reports to the Governance Committee on an annual basis, unless exceptional circumstances indicate otherwise.

The Information Asset Owner is the senior person assigned the overall responsibility for security and integrity of Information Assets, e.g. HR databases/CRM systems.

Appendix A: Terms of Reference (Information Governance Steering Group)

Purpose / role of the group:

The Information Governance Steering Group (IGSG) will identify and inform all aspects of the Association's approach to the safe storage, handling and sharing of information in order to comply with relevant legislation and guidance.

The IGSG will support the investigation of incidents in the event of a data protection breach, near miss or complaint.

The IGSG will inform and shape the governance of information across the Association by:

- Highlighting and acting on threats and risks through sources such as data breaches and complaints noting trends and capturing near-misses.
- Reviewing the information governance policy every three years (or by exception) and ensure alignment with related policies and procedures.
- Supporting the design and the implementation of training, or opportunities for learning, ensuring that all employees and volunteers understand and are equipped to comply with Information Governance processes and procedures.
- Identifying and sharing best practice across the Association (where appropriate).
- Ensuring the monitoring and enforcement of records management, retention and disposal procedures.
- Ensuring all members of the IGSG have up-to-date knowledge of current legislation.
- Representing all teams through the membership and ensuring all members take responsibility for communicating and proactively deploying developments and change within their teams.
- Reporting findings and actions to Directors team and to the Governance Committee
- Ensuring clear and concise communication to key stakeholders through the most appropriate medium (SharePoint/The News/website).
- Ensuring that any undertakings of the Association are considered in the context of the differing England, Northern Ireland and Wales democratic structures, issues are identified and appropriate actions taken.

Membership:

Director of Fundraising – Senior Information Risk Officer
Assistant Director of Care
Head of ICT
Head of Communications & Digital
Head of Human Resources
Head of Volunteering
Head of Data & Insight
A representative from each directorate (Regional Care, National Care, Research, CEO, Policy & Campaigns, Partnerships/Education/Information)

Representation from each team identified above is important for the governance of information within the Association. A deputy must attend the meeting if a member is unable to be present.

Accountability:

Directors' Team, Governance Committee

Review:

- Review of the relevance and value of the IGSG work and the terms of reference every two years, or by exception
- Annual report to Governance Committee (in February)

Meetings:

- Meetings will be held quarterly in Northampton or by Teams and chaired by Director of Fundraising
- Meetings including agenda items, minute taking, circulation and storage will be managed by the Governance Officer.
- Non-members will be invited where topics or task and finish groups indicate their expertise and knowledge would be beneficial

Sharing of information and resources:

- Confidential materials stored on SharePoint will be password protected

Definition of terms:

- Definition of any key terms are captured within the Information Governance Policy and other associated policies