

Data Protection, Data Management, and Confidentiality Policy

Version: 2.0

Date: 21.01.2026

Endorsed by Manas Board of Trustees

Application: This policy applies to the personal data of site visitors, research participant, clients, partners / collaborators, prospective applicants, employees (workers, contractors), volunteers, interns, and consultants contracted.

Applies to: All staff, consultants, researchers, trainers, supervisors, and partners working with Manas.

Section I. Background

Manas is an international organisation specialising in trauma-informed mental health and psychosocial support (MHPSS) approaches for justice, recovery, research, and learning. Our work includes research, documentation, training, supervision and advisory services. We do not provide direct clinical or therapeutic services.

Purpose: This policy sets out how Manas collects, uses, stores, shares, and protects data, ensuring that all activities are conducted ethically, safely, and in line with international data protection and research standards.

Manas is committed to being transparent about how it collects and uses the personal data it collects, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to Manas, a not-for-profit company registered in England and Wales with Companies House as Manas with registration number **15524729**, whose registered address is:

5 Brayford Square
London
E1 0SG

Responsibilities:

- The organisation has appointed *Dr Dean Flanagan* as its data protection focal point. Their role is to inform and advise the organisation on its data protection obligations. They can be contacted at Dean@manas.org.uk. Questions about this policy, or requests for further information, should be directed to the data protection officer.
- Project supervisors and coordinators are responsible for ethical data management within their projects.
- All staff and consultants must comply with this policy.
- Partners handling Manas data are expected to meet equivalent standards.

Core Principles: All data handling by Manas is guided by the following principles:

1. **Do no harm** – data practices must not place individuals or communities at risk.
2. **Trauma-informed practice** – data collection and use must recognise power, vulnerability, consent, and safety.
3. **Confidentiality and dignity** – individuals’ information is treated with respect and care.
4. **Data minimisation** – only data that is necessary for the stated purpose is collected.
5. **Transparency** – participants are informed how their data will be used.
6. **Accountability** – responsibility for data protection is clearly assigned.
7. **Proportionality** – safeguards match the sensitivity and risk level of the data.

Overall approach: Manas follows a strict policy when it comes to confidentiality and the management of sensitive data, whether this relates to research or clinical data gathered through our activities. All MHPSS experts must adhere to the policy of the regulated professional body to which all clinicians are registered under in each of the country of practice (i.e. Medical council, HCPC, etc). As a UK-based organisation, Manas particularly follows the standards set out by the UK Health & Care Professions Council [HCPC]: <https://www.hcpc-uk.org/standards/>

In terms of record keeping, our overall standard is that the organisation should keep and maintain records for all service users and clients that are:

- Clear and accurate;
- In accordance with applicable legislation, protocols, and guidelines;
- Completed as soon as possible; and
- Kept safe from being lost, damaged, or accessed inappropriately.

Section II. Specifics on data collected

Scope of Data: This policy applies to all data handled by Manas, including:

- Research data
- Training and supervision materials
- Monitoring, evaluation and learning (MEL) data
- Documentation and case-based analysis
- Administrative and partner data

Types of Data Collected: Depending on the project, Manas may collect or generate:

- Qualitative data: interviews, focus groups, field notes, observations
- Audio or audiovisual recordings: where explicitly consented
- Textual data: transcripts, reports, coded datasets
- Training data: attendance records, feedback forms, learning reflections
- Secondary data: publicly available documents, reports, or datasets

Manas avoids collecting direct clinical, diagnostic or therapeutic data.

Personal data: Some projects may involve personal or sensitive data, including:

- Experiences of violence, trauma, or injustice
- Politically, legally or culturally sensitive information
- Professional or institutional roles of participants

Where such data is involved, additional safeguards apply (see following sections).

Lawful and ethical data use: Manas processes data based on one or more of the following:

- Informed consent of participants
- Legitimate research, learning or documentation purposes
- Contractual or donor requirements, where applicable

All research involving human participants follows recognised ethical research principles and, where required, obtains approval from appropriate ethics bodies or institutional review processes.

Informed consent: Where Manas collects data from individuals:

- Participation is voluntary
- Participants are informed about:
 - What data is collected
 - Why it is collected
 - How it will be used and stored
 - Who may have access
 - Their right to refuse, withdraw, or request deletion where feasible

- Consent may be written or verbal, depending on context and risk
- Special care is taken in contexts of vulnerability, insecurity, or power imbalance.

Anonymisation and confidentiality: To protect participants, the organisation will implement the following:

- Data is anonymised or pseudonymised wherever possible
- Direct identifiers are removed from transcripts and reports
- Identifying details are generalised or concealed in publications
- Where full anonymity is not possible, this is clearly explained to participants

Confidentiality commitments are respected unless disclosure is required by law or necessary to prevent serious harm.

Data storage and security: Manas uses risk-appropriate technical and organisational measures, including:

- Password-protected devices and accounts
- Encrypted storage for sensitive data
- Restricted access based on role and necessity
- Secure file-sharing platforms for partner collaboration through Dropbox.
- Regular backups

Dropbox is the main server Manas is using to store data. Highly sensitive personal data is not stored on unsecured or public cloud services.

Data access and permission:

- Access is limited to authorised staff or collaborators
- Roles and responsibilities for data access are defined per project
- Sensitive datasets are shared strictly on a need-to-know basis
- Where relevant, data-sharing agreements or confidentiality clauses are used

Data retention and deletion: Data is retained only as long as necessary for the stated purpose. Retention periods consider:

- Ethical obligations
- Donor or institutional requirements
- Safety and confidentiality risks

Data is securely deleted or archived once no longer required.

Data sharing and publications: Manas may share or publish data in:

- Research reports and publications
- Learning materials and training outputs
- Policy briefs and documentation

All shared outputs are reviewed to ensure:

- No unnecessary identification of individuals or communities
- Risks of harm are minimised
- Consent conditions are respected

International and cross-border work: As an international organisation, Manas operates across multiple legal and cultural contexts. We aim to align with:

- International data protection principles (including GDPR-aligned standards where applicable)
- Ethical research guidance relevant to humanitarian, justice and MHPSS contexts
- Local legal requirements where data is collected

Any breaches or concerns: Any actual or suspected data breach, loss, or misuse must be reported immediately to Manas leadership so that risks can be assessed and mitigated.

Section III – Responsibility of Manas team and staff

We are legally required to keep all our data secure. Consultants must work in accordance with this Policy when handling personal data in the course of employment including personal data relating to any employee, worker, collaborator, funder, client, supplier of the company.

As a consultant working on behalf of Manas, and all staff working or volunteering for Manas commit to:

- Ensure proper and secure storage of any personal data gathered from Manas clients, and other beneficiaries the Consultant engages with during the term of the Contract
- Inform Manas at the earliest possible opportunity if any confidential information, including personal data, is lost or stolen
- Not share any personal data gathered in the course of the engagement and beyond with Manas without Manas' express written permission
- Destroy any personal data gathered through the work upon provision of the deliverables
- Not make public any information relating to the activities of Manas and its clients or the work performed under contract with Manas without prior consent from Manas and clients
- Ensure that any public mention of the work conducted under this contract acknowledges Manas appropriately.

Section IV. Data privacy on Manas website

User Type:

- Site Visitor: You are a site visitor when you visit and interact with our web sites, web pages, blogs and content on [www.manas.org.uk]
- Research Participant: You are a Research Participant when you have agreed to take part in research that Manas is conducting.
- Client: You are paying to use the services of Manas.
- Consultant / Partner / Collaborator: You are an existing Partner or Collaborator once you have engaged with Manas in a contract.
- Prospective Applicant: You are a Prospective Applicant when you apply to a position at Manas.
- Employee: You are working as an employee at Manas.
- Former employee: You have previously been an employee at Manas.

Principles

There are six principles for which all personal data must be processed according to [Article 5](#) of the GDPR. These principles outline what any company that has a digital presence needs to keep accountable towards:

1. Lawfulness, fairness, and transparency: Obey the law, only process personal data in a way that people would reasonably expect, and always be open about your data protection practices.
2. Purpose limitation: You must normally only process personal data for the specific reason you collected it and nothing else.
3. Data minimization: don't process any more data than you need.
4. Accuracy: make sure that any personal data you hold is adequate and accurate.
5. Storage limitation: don't store personal data for longer than you need to.
6. Integrity and confidentiality: always process personal data securely.

These principles build the foundation for why data is being collected and all of the data that Manas is collecting falls in line with one of these six principles.

1. Collection of personal information about visitors to the website

1.1. When given to us directly

For example, personal information that they submit through our website or personal information that they give to Manas when they communicate with us by email, phone or letter.

1.2. When Manas obtains it indirectly

For example, their personal information may be shared with Manas by third parties, including sub-contractors in technical and delivery services; analytics providers and search information providers. To the extent we have not done so already, we will notify

them when we receive personal information about them from the third party and will tell them how and why we intend to use that personal information.

1.3. When it is available publicly

Their personal information may be available to us from external publicly available sources. For example, depending on the visitors privacy settings for social media services, we may access information from those accounts or services (for example when you choose to interact with us through platforms such as Facebook, Instagram or Twitter).

1.4. When visitors visit our website

The information we will process includes: 1. Their name and their email address. 2. The details of when/where we communicate.

Whenever we process data for these purposes, we will ensure that we always keep their Personal Data Rights in high regard and take account of these rights.

Why do we hold this personal data?

To provide communications which Manas thinks will be of interest to them. For the purposes of marketing, we will keep your data unless requested otherwise.

What processing conditions do we use to process such personal data?

We may process visitors' personal information for carefully considered and specific purposes which are in our interests and enable us to enhance the services we provide.

Who do we share this personal information with?

Personal data of our contacts is shared only within our organisation.

What are visitors' rights relating to the information we hold about them?

They have certain rights with regards to the data we hold on them and how we use it. They can request to see a copy of the data we hold on them. They have the right change any of the data we hold about them if it is inaccurate. They also have the right to request that we delete any data that we hold on them if it is no longer relevant or necessary for us to use.

Do this by email: info@manas.org.uk or post: Manas International Ltd, 5 Brayford Square, London, E1 0SG. UK

1.5. We also collect and use such personal information by using cookies on our website – please see our cookie policy.

In general, we may combine this personal information from these different sources for the purposes set out in this Policy.

2. What personal information do we use?

2.1. We may collect, store and use the following kinds of personal information:

- name and contact details (postal address, email address);
- information about your computer/mobile device and your visits to and use of our website, including, for example, your IP address and geographical location;
- details of your qualifications and experience;
- date of birth and gender; and/or
- any other personal information which we obtain as per clause 1.

2.2. The EU General Data Protection Regulation (“GDPR”) recognises certain categories of personal information as sensitive and therefore requiring more protection, for example information about your health, ethnicity and political opinions. In certain situations, we may collect and/or use these special categories of personal information (for example, health information to ensure equal access). We will only process these special categories of personal information if there is a valid reason for doing so and where the GDPR allows us to do so.

3. How and why will we use such personal information?

The personal information, however provided to us, will be used for the purposes specified in this Policy. In particular, we may use visitors’ personal information:

- to provide services, products and information you have requested;
- to communicate in relation to the work of Manas;
- to provide further information about Manas’s work, services, activities and/or products (where necessary, only where consent has been provided to receive such information);
- to communicate about a project you are involved in;
- to analyse and improve our work, services, activities, products and/or information (including for our website), and/or for our internal records;
- to report on the impact and effectiveness of our work;
- to publish news articles and other information on our website;
- to process application for a job with us when you apply through our website;
- to administer employment/other working relationship with us (for example, to pay your salary);
- to provide references, for example to landlords and new employers; for training and/or quality control;
- to audit and/or administer our accounts;
- to satisfy legal obligations which are binding on us, for example in relation to regulatory, government and/or law enforcement bodies with whom we may work

(for example requirements relating to the payment of tax or anti-money laundering);

- for the prevention of fraud or misuse of services; and/or
- for the establishment, defence and/or enforcement of legal claims.

4. Communications for marketing

4.1. We may use contact details to provide information about our work, events, services and/or products which we consider may be of interest to you (for example, information about future work). Where we do this via email, SMS or telephone, we will not do so without your prior consent (unless allowed to do so via applicable law).

4.2. Where you have provided us with consent previously but do not wish to be contacted by us about our work, events, services and/or products in the future, you may opt out of receiving emails from us at any time by clicking the “unsubscribe” link and the bottom of our emails; or by contacting us at info@manas.org.uk

5. How long do we keep personal information?

5.1. In general, unless still required in connection with the purpose(s) for which it was collected and/or processed, we remove personal information from our records six years after the date it was collected.

5.2. However, if before that date (i) personal information is no longer required in connection with such purpose(s), (ii) we are no longer lawfully entitled to use it or (iii) you validly exercise your right of erasure (please see section 11 below), we will remove it from our records at the relevant time. We review personal information that we hold at least annually in order to verify if it is still validly required in connection with the purpose(s) for which we collected it.

6. Will we share your personal information?

We will not sell or rent your personal information with third party organisations. However, in general we may disclose your personal information to selected third parties in order to achieve the purposes set out in this Policy. Non-exhaustively, those parties may include:

1. suppliers and sub-contractors for the performance of any contract we enter into with them, for example IT service providers such as cloud storage providers or mailing houses;
2. professional service providers such as accountants and lawyers;
3. parties assisting us with research to monitor the impact/effectiveness of our work;
4. regulatory authorities, such as tax authorities; and/or
5. analytics and search engine providers.

7. Security/storage of and access to personal information

We are committed to keeping personal information safe and secure and we have appropriate and proportionate security policies and organisational and technical measures in place to help protect personal information. Personal information is only accessible by appropriately trained staff, and stored on secure servers with features enacted to prevent unauthorised access.

8. Exercising rights

8.1. Where we rely on consent to use personal information, individuals have the right to withdraw that consent at any time. This includes the right to ask us to stop using personal information for marketing purposes or to unsubscribe from our email list at any time. They have the following rights:

- Right of access – individuals or organisations can write to us to ask for confirmation of what personal information we hold on you and to request a copy of that personal information. Provided we are satisfied that they are entitled to see the personal information requested and we have successfully confirmed the identity, we will provide with your personal information subject to any exemptions that apply.
- Right of erasure – at request we will delete the personal information from our records as far as we are required to do so.
- Right of rectification – if they believe our records of their personal information are inaccurate, they have the right to ask for those records to be updated. They can also ask us to check the personal information we hold if they are unsure whether it is accurate/up to date.
- Right to restrict processing – they have the right to ask for processing of your personal information to be restricted if there is disagreement about its accuracy or legitimate usage.
- Right to object – they have the right to object to processing where we are (i) processing personal information on the basis of the legitimate interests basis (see paragraph 4), (ii) using personal information for direct marketing or (iii) using information for statistical purposes. If they object to direct marketing, we will retain certain limited personal information about you to ensure that we do not contain them again.
- Right to data portability – to the extent required by the GDPR, where we are processing personal information (that you have provided to us) either (i) by relying on consent or (ii) because such processing is necessary for the performance of a contract to which they are a party or to take steps at their request prior to entering into a contract, and in either case we are processing using automated means (i.e. with no human involvement), they may ask us to provide the personal information to you – or another organisation – in a machine-readable format.

- Rights related to automated decision-making – they have the right not to be subject to a decision based solely on automated processing of your personal information which produces legal effects or similarly significantly affects them, unless such a decision (i) is necessary to enter into/perform a contract between you and us/another organisation; (ii) is authorised by EU or UK law (as long as that law offers you sufficient protection); or (iii) is based on your explicit consent.

8.2. Please note that some of these rights only apply in limited circumstances.

8.3. We encourage raising any concerns or complaints about our data processing by contacting us using the details provided in section 14 below. They are further entitled to make a complaint to the Information Commissioner’s Office – www.ico.org.uk.

9. Links and third parties

Manas website may contain links to other websites. We are not responsible for the privacy policies or practices of third-party websites.

10. Review of Privacy Policy

This Policy will be reviewed periodically and updated as needed to reflect changes in Law, best practice or organisational activities. We will notify the concerned entities when relevant of any significant changes where reasonably possible for us to do so and by placing an updated notice on our website. The document was last updated in **January 2026**.

Overall policy review and update

This policy is reviewed periodically and updated as needed to reflect changes in law, best practice, or organisational activities.

Contact

For questions related to data protection or confidentiality, contact the data protection focal point in the organisation: *Dr Dean Flanagan*. They can be contacted at Dean@manas.org.uk.