Policy Name	**PRIVACY AND COOKIES**
Approved by	**INFORMATION GOVERNANCE WORKING GROUP**
Responsible Person	**DATA PROTECTION OFFICER**
Date of Approval	**February 2026**
Next Review Date	**MAY 2028**
Staff notified of updated policy and where this can be located	**2026 / NWM Website / Internal HR System**
Who does this Policy Apply to?	**TRUSTEES, STAFF, GENERAL PUBLIC**
This policy will be reviewed in accordance with the designated review schedule. It will remain live & active until such time as the review prompts necessary changes.	

Version	Date	Author	Rationale
1.1	24/10/2025	IG & Data Manager	Conducting a review of 2024 policy to ensure it aligns with up-to-date ICO guidance and current N&WM data practices and systems. Review informed by other Mind policies, online legal GDPR resources and ICO guidance.
1.2	24/11/2025	IG & Data Manager	Reviewing content after initial proposal to IG working group – changing the order, formatting, and removing reference to reliance on healthcare for lawful basis.
1.3	11/12/2025	Junior Reporting Analyst	Reviewing language and formatting.
1.4	18/12/2025	IG & Data Manager	Final review for proposal to IG working group.
1.5	20/02/2026	IG Working Group	Reviewed following legal guidance.

1. Policy Statement

1.1. This policy sits within the Information Governance Suite of policies. All within this suite are approved by the Information Governance Working Group of Norfolk and Waveney Mind (hereafter referred to as "**N&WM**", "**the organisation**", "**we**", "**us**", "**our**").

1.2. N&WM is committed to protecting the privacy and personal data of anyone who engages with the organisation, including service users, staff, and supporters.

1.3. This policy explains what personal data we collect, how we use it, and the data subject's rights under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (together referred to as "**data protection law**").

1.4. This policy will be made available to all persons engaging with the organisation and will be published on the organisation's public facing website.

2. Aims

2.1. The aim of this policy is to set out how N&WM collects, uses and protects personal data and ensures compliance with data protection law.

2.2. We want everyone who engages with us—whether for support, employment, volunteering, or fundraising—to feel confident that their personal data is handled lawfully, securely, and with respect.

2.3. Specifically, this policy aims to:

- Explain how and why we collect, use, and share personal data.
- Provide assurance that we only process personal data for legitimate purposes and with appropriate safeguards.
- Make it easy for individuals to understand and exercise their rights.
- Confirm that we will never share personal data with third parties for their own marketing purposes.
- Outline our commitment to transparency, security, and ethical data handling.

3. Scope

3.1. This policy covers all personal data collected by the organisation for the following purposes:

- Provision of Mental Health services
- Staff recruitment and management
- Volunteering activities and volunteer management
- Marketing including fundraising, campaigning and membership services
- Training
- Monitoring, evaluation and audit of service provision

3.2. To ensure transparency and compliance with data protection law, we will publish clear and concise summaries of our Privacy Policy in the form of privacy notices tailored to each category of data subject. These categories, as defined in section 7.2, include employees, volunteers, service users, donors, and website visitors.

- Each privacy notice will outline the key elements of data processing relevant to that category, including the types of personal data collected, the purposes for processing, the lawful basis under applicable legislation, retention periods, and the rights available to individuals.
- Both the full Privacy Policy and the individual privacy notices will be made accessible on our website and will be subject to regular review and updates to reflect any changes in our data processing activities or legal requirements.

4. Who we are and contact details

4.1. N&WM is the controller for personal data processed in connection with our services, operations, and activities, with the exception of data which is stored on any systems managed by commissioners of our services. This means that N&WM determines the purposes and means of processing personal data, in accordance with data protection law.

4.2. N&WM is registered with the Information Commissioners Office and the organisation's registration number is Z4761485.

4.3. The organisation has appointed a Data Protection Officer who is responsible for overseeing questions in relation to this policy. Any queries related to this policy should be directed to our Data Protection Officer using the following details:

Data Protection officer,
Norfolk and Waveney Mind,
50 Sale Road, Norwich, Norfolk NR7 9TP

DPO@norfolkandwaveneymind.org.uk

5. How we collect information

5.1. We might collect information about you in the following ways:

- **When you interact with us directly**. This might occur in the following circumstances (amongst others): if you contact us in person, on the phone, via a letter, or digitally; if you register with us for training or an event; if you donate to us; if you complete feedback or a survey for us; if you self-refer to our services; and/or through communication with us during support we provide to you.
- **When you interact with us through partners or suppliers working with or on our behalf.** This might be if you are referred to us through another organisation or partner, or if another organisation contacts us about you and/or your care.
- **When you visit our website.** We gather general information which might include pages you visit most often and which services, events, or information is of most interest to you. We also use "cookies" to help our site run effectively.

6. What personal data we collect and our lawful basis for using that personal data

6.1. "**Personal data**" means any information about an individual from which that person can be identified. It does not include information from which the person's identity has been removed (anonymous data).

6.2. The types of personal data N&WM collects about individuals depends on the reason for the individual engaging with us. For example, for someone receiving mental health support we may collect their NHS number, but we would not hold this for a member of staff. Further details about the types of personal data we collect for various categories of data subject can be found in the table at paragraph 6.5 below, as well as in our summaries of this policy which are tailored to each category of data subject.

6.3. Under data protection law, we must have a "lawful basis" for collecting and using personal data. There is a list of possible lawful bases in the UK GDPR. The data subject can find out more about lawful bases on the ICO's website.

6.4. Our lawful bases for collecting or using personal data will fall into the following categories, depending on the personal data collected and the purpose for which it is being processed. .

- **Legitimate interest –** We process data when it is necessary to support our legitimate activities, or those of a third party, without causing undue risk or harm to individuals.
- **Consent –** We process data when the data subject has given clear and informed permission for a specific purpose. Where this lawful basis has been used, please note that the data subject can withdraw their consent at any time by contacting dpo@norfolkandwaveneymind.org.uk
- **Contract –** this is where the organisation has entered into (or is about to enter into) a contract which requires us to process the personal data in order to comply with the contract. For example, a contract of employment requires us to process the employee's personal data in order to pay the employee their salary.
- **Legal obligation –** this is where the organisation is obliged to process personal data to comply with the law.

6.5. The table below provides a summary of what personal data we collect, why we collect it, and the lawful basis for doing so. For a full detailed record of processing activities, please contact dpo@norfolkandwaveneymind.org.uk. Note that any data which is a protected characteristic is stored on the basis of consent and this consent can be revoked at any time.

Data Subject Category	Personal Data Items	Purpose	Lawful basis	Special category lawful basis
Service users	Full name, pronouns, contact details	Service and support delivery, communication, onward referrals	Legitimate Interest	
Service users	Protected characteristics	Equality monitoring, service improvement	Consent	(Art. 9(2)(a)) Explicit Consent

Data Subject Category	Personal Data Items	Purpose	Lawful basis	Special category lawful basis
Service users	Mental health data	Service and support delivery, safeguarding, NHS reporting	Legitimate Interest	Art. 9(2)(g) – Substantial Public Interest (Safeguarding), DPA 2018 Schedule 1 paragraph 18. Where support is delivered by qualified health or counselling professionals, Art. 9(2)(h) (health and social care) may also apply.
Service users	Physical health data	Service and support delivery, safeguarding	Legitimate Interest	Art. 9(2)(g) – Substantial Public Interest (safeguarding) – DPA 2018 Sch. 1 para 18
Service users	Personal identifiers e.g., NHS number	Service and support delivery, onward referrals	Legitimate Interest	Art. 9(2)(g) – Substantial Public Interest (safeguarding) – DPA 2018 Sch. 1 para 18 (if combined with health data)
Service users	Additional contacts e.g., next of kin, referrer, emergency contact	Emergency contact, safeguarding	Legitimate Interest	
Staff and trustees	Full name, pronouns, contact details	Recruitment, HR records, payroll	Contract / Legal Obligation	
Staff and trustees	Protected characteristics	Equality monitoring	Consent	(Art. 9(2)(a)) Explicit Consent
Staff and trustees	Mental health data	Occupational health, absence management, training	Legal Obligation	(Art. 9(2)(b) Employment, social security and social protection law
Staff and trustees	Physical health data	Occupational health, absence management, training	Legal Obligation	(Art. 9(2)(b) Employment, social security and social protection law
Staff and trustees	Personal identifiers e.g., NI number	Right to work checks, payroll	Legal Obligation	
Staff and trustees	Additional contacts e.g., next of kin, referrer, emergency contact	Emergency contact	Legitimate Interest	

Data Subject Category	Personal Data Items	Purpose	Lawful basis	Special category lawful basis
Staff and trustees	Financial information	Payroll, pensions	Contract / Legal Obligation	
Staff and trustees	Right to work and other supporting documents, for example for DBS checks	Recruitment compliance	Legal Obligation	(Art. 9(2)(b) Employment, social security and social protection law
Donors and fundraisers including ticket purchasers	Full name, pronouns, contact details	Donation management, communication	Legitimate Interest	
Donors and fundraisers including ticket purchasers	Donation data	Processing donations, Gift Aid	Legal Obligation (Gift Aid) / Legitimate Interests (other donation processing)	
Event attendees	Full name, pronouns, contact details	Event registration	Legitimate Interest	
Event attendees	Photographs and videos	Marketing, event records	Consent	
Training attendees	Full name, pronouns, contact details	Training registration	Legitimate Interest / Contract	
WiFi users	IP addresses, Cookies and digital IDs	Network security, analytics	Legitimate Interest	
Site visitors	CCTV footage	Security, crime prevention	Legitimate Interest	
Site visitors	Sign in logs	Safety, compliance	Legal Obligation	
Website and digital visitors/followers	IP addresses, Cookies and digital IDs	Analytics, site functionality	Legitimate Interest	
Feedback /survey respondee	Full name, contact details	Service improvement	Legitimate interest	

Data Subject Category	Personal Data Items	Purpose	Lawful basis	Special category lawful basis
Complainant	Full name, pronouns, contact details	Complaint handling, service improvement	Legal Obligation	Art. 9(2)(f) applies where a legal claim is in contemplation or likely. Art. 9(2)(g) + DPA Sch1 para 18 applies where safeguarding is involved.
Subject of incident or accident	Full name, contact details, contents of other records to support investigations	Investigation	Legal Obligation	Art. 9(2)(f) applies where a legal claim is in contemplation or likely. Art. 9(2)(g) + DPA Sch1 para 18 applies where safeguarding is involved.
Subject referenced in email	Email data	Communication, audit	Legitimate Interest	Special category data may be processed incidentally. Where this occurs, relevant Art. 9 conditions apply (e.g., safeguarding or legal claims).
Subject referenced in files	Personal data in files	Business continuity, audit	Legitimate Interest	Special category data may be processed incidentally. Where this occurs, relevant Art. 9 conditions apply (e.g., safeguarding or legal claims).
Enquiries into ticketing systems	Full name, pronouns, contact details	IT/HR/Assurance/Estates/Payroll support	Legitimate Interest	
Individuals contacting by telephone	Call recordings	Quality assurance, safeguarding	Legitimate Interest	Art. 9(2)(g) – Substantial Public Interest (safeguarding) – DPA 2018 Sch. 1 para 18 and/or Art. 9(2)(f) Legal claims and judicial acts
Video call participants	Video call recordings	Internal information sharing, business continuity and investigations	Legitimate Interest	Art. 9(2)(g) – Substantial Public Interest (safeguarding) – DPA 2018 Sch. 1 para 18 and/or Art. 9(2)(f) Legal claims and judicial acts

7. Data Subject Rights

7.1. As a data subject, you have various rights in respect of the personal data the organisation holds about you.

7.2. Which lawful basis we rely on may affect the rights which are set out in brief below. More information about data subject rights and the exemptions which may apply can be found on the ICO's website: https://ico.org.uk/global/privacy-notice/your-data-protection-rights/. For further information about individual rights, please contact DPO@norfolkandwaveneymind.org.uk.

- **The right of access** - You have the right to ask us for copies of your personal data, details about where we get personal data from, and who we share personal data with.
- **The right to rectification** - You have the right to ask us to correct personal data if you think it is inaccurate or incomplete, however we may need to verify the accuracy of the new data you provide to us.
- **The right to erasure** – In certain circumstances, you have the right to ask us to delete your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- **The right to restriction of processing** – You have the right to ask us to limit how we can use your personal data in one of the following scenarios:
  - if you want us to establish the data's accuracy;
  - where our use of the data is unlawful, but you do not want us to erase it;
  - where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
  - you have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.
- **The right to object to processing** - You may have the right to object to the processing of personal data where we are relying on a legitimate interest (or those of a third party) as the legal basis for that particular use of your data (including carrying out profiling based on our legitimate interests). In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your right to object.
- **The right to data portability** - You have the right to ask that we transfer the personal data you gave us to another organisation, or to them directly.
- **The right to withdraw consent** – When we use consent as our lawful basis the data subject may have the right to withdraw consent at any time. Please note that this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain services to you and we will advise you if this is the case at the time you withdraw your consent.

7.3. All requests to exercise any data subject rights should provide evidence of identity or consent to receive data. Data will only be shared, or requests actioned, when appropriate evidence of identification has been provided and when the scope of the request has been formalised.

7.4. If the data subject makes a request to exercise any of the rights set out above, N&WM will make an initial response without undue delay and, in any event, within one month.

The completion of the request will be within one month of receipt of verification of the data subject's identity and confirmation of the validity and scope of the request. We will follow ICO guidance to assess whether a request is reasonable and to determine the appropriate course of action if it is not, and will keep the data subject informed of steps at every possible opportunity.

7.5. Please note that the above rights are only applicable if we have collected and stored personal data. This above does not apply to anonymous data, such as anonymous feedback.

8. Data sharing and disclosure

8.1. The personal data we collect about any data subject will mainly be used by our staff and volunteers.

8.2. Please note that data in our electronic systems may be accessed by both support and administrative staff to enable the safe delivery of support and communication, subject to appropriate role-based access.

8.3. We will never sell or share personal data, including web browsing activity, with organisations so that they can contact the data subject for any marketing activities.

8.4. In some cases, N&WM will use third party data processors to manage systems which hold personal data. Where third party data processors are used, processing of information is always carried out under our instruction and N&WM will have up to date contractual agreements in place that require partners to comply with data protection law and ensure that they have appropriate controls in place to secure information. To find out more about the third party data processors we use, please contact dpo@norfolkandwaveneymind.org.uk

8.5. Where personal data is processed in a new way, N&WM will conduct an initial screening to determine whether a Data Protection Impact Assessment (DPIA) is required. If a DPIA is necessary, it will be completed in accordance with regulatory requirements. A list of completed DPIAs will be published on our website, alongside details of the data processors and handlers engaged in our processing activities. Copies of individual assessments are available upon request by contacting dpo@norfolkandwaveneymind.org.uk.

8.6. National opt-out: Some of our NHS-funded services require N&WM to submit personal data to the NHS Mental Health Services Data Set which is mandatory. However, the national data opt-out process allows service users to have some control by setting opt-out preferences for how data is used by NHS Digital. Individuals can opt out by utilising the NHS opt out service: https://digital.nhs.uk/services/national-data-opt-out

8.7. Duty of confidentiality: We are subject to a common law duty of confidentiality, which means we cannot share personal data without some form of legal authority or justification. However, there are some circumstances where we can and will share relevant health and care information. These are where:

- The data subject has provided us with their consent (either where N&WM have taken it as implied to provide the data subject with care, or the data subject has provided it explicitly for other uses);
- We have a legal requirement (including court orders) to collect, share or use the data;

- On a case-by-case basis, the public interest to collect, share and use the data overrides the public interest served by protecting the duty of confidentiality (for example sharing information with the police to support the detection or prevention of serious crime);
- We are acting in line with legitimate interests. In this circumstance we will carry out and document a Legitimate Interest Assessment.
- If in England or Wales – the requirements of The Health Service (Control of Patient Information) Regulations 2002 are satisfied; or
- If in Scotland – we have the authority to share provided by the Chief Medical Officer for Scotland, the Chief Executive of NHS Scotland, the Public Benefit and Privacy Panel for Health and Social Care or other similar governance and scrutiny process.

8.8. Legal disclosure: We may disclose the data subject information if required to do so by law (for example, to comply with applicable laws, regulations and codes of practice or in response to a valid request from a competent authority); or, in order to enforce our conditions of sale and other agreements.

9. Keeping the data subject's information safe

9.1. We take looking after personal data very seriously. We've implemented appropriate physical, technical and organisational measures to protect the personal data we have under our control, both on and off-line, from improper access, use, alteration, destruction and loss.

9.2. We aim to maintain compliance and accreditation with Cyber Essentials+ and the NHS DSPT (data security protection toolkit) so that data subjects can be confident their personal data is handled securely.

9.3. Staff receive annual Data Security Awareness training and are unable to access N&WM systems until this is completed.

9.4. We log all data security incidents and breaches to ensure that we handle all incidents appropriately and learn from them.

9.5. Our websites may contain links to other sites. While we try to link only to sites that share our high standards and respect for privacy, we are not responsible for the content or the privacy practices employed by other sites. Please be aware that advertisers or websites that have links on our site may collect personally identifiable information about the data subject. This privacy policy does not cover the information practices of those websites or advertisers.

9.6. Any debit or credit card details submitted through our website are transmitted securely to our payment processing partners in accordance with the Payment Card Industry Data Security Standards (PCI DSS). We do not store any card details on our systems.

9.7. N&WM will conduct and report the results of regular system audits to ensure that, where N&WM staff have access to records, they are only being accessed in an appropriate way.

9.8. International Transfers

N&WM does not routinely transfer personal data outside the UK. Personal data is

stored and processed within the UK or in locations that comply with UK data protection law. If in future we need to transfer personal data internationally, we will ensure that appropriate safeguards are in place, such as:

- Transfers only to countries with an adequacy decision from the UK Government;
- Use of standard contractual clauses approved by the Information Commissioner's Office;
- Additional technical and organisational measures to protect the data subject's data

10. Children and young people

10.1. In some services, we may be the controller for personal data relating to children and young people. In accordance with data protection law, a child is anyone under the age of 18.

10.2. When we refer to someone with parental responsibility for a child we mean someone who, according to the law in the child's country of residence, has the legal rights and responsibilities for a child that are normally afforded to parents. This will not always be a child's 'natural parents' and parental responsibility can be held by more than one natural or legal person.

10.3. Where the data for children and young people is held, it will be done using the lawful basis of Substantial Public Interest (Safeguarding), or consent. If consent is relied upon and the child is under the age of 13, parental consent will be sought. Otherwise, consent will come from the young person directly and NWM will ensure that this is explained using material with clear, age-appropriate language.

10.4. Young people have the same rights under data protection law as adults.

10.5. In some cases, a parent or guardian may apply for access to young person's information.

- If a young person does not consent, we may not provide access to the adult.
- If the young person does not have the capacity to understand, we may provide access to the adult because it is in the young person's best interest to do so.
- Young people can ask us to keep certain parts of their information confidential.

10.6. If the young person is making decisions about their information that puts them at risk, we may notify adults with parental rights.

11. Cookies

11.1. A 'cookie' is a name for a small file, usually of letters and numbers, which is downloaded onto the user's device, like a computer, mobile phone or tablet when they visit a website.

11.2. Cookies let websites recognise a device, so that the sites can work more effectively, and also gather information about how the user uses the site. A cookie, by itself, can't be used to identify an individual.

11.3. When a person visits our website, N&WM gathers general information which might include which pages they visit most often and which services, events or information is of most interest to the individual. N&WM may also track which pages they visit when they

click on links in emails from us. We also use cookies to help our site run effectively.

11.4. N&WM use three distinct categories of cookie on our website:

- Strictly Necessary cookies are essential for the user to move around our website and to use its features.
- Performance cookies collect anonymous information about how the user uses our site, like which pages are visited most.
- Functionality cookies collect anonymous information that remember choices the user make to improve their experience, like text size or location. They may also be used to provide services the user has asked for such as watching a video or commenting on a blog.

11.5. Users can opt out of all our cookies (except the Strictly Necessary ones). People can find out how to control and delete cookies in their browsers. But, should users choose to refuse all cookies, our website may not function for them as we would like it to.

12. Data Retention

12.1. We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

12.2. To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

12.3. N&WM has a robust Data Retention Policy stating the timescales for how long we will retain different categories of personal data.

12.4. The Data Retention Policy is available by request from the organisation's Data Protection Officer (see paragraph 4.3 above for contact details of the Data Protection Officer)

13. Complaints

13.1. If any data subject wishes to make a complaint or raise a concern regarding data protection, they can contact us at

Data Protection officer,
Norfolk and Waveney Mind,
50 Sale Road, Norwich, Norfolk NR7 9TP

DPO@norfolkandwaveneymind.org.uk

13.2. Should it be necessary - Complaints can be made to the data protection supervisory authority, the Information Commissioner's Office: https://ico.org.uk

13.3. Before contacting the ICO, we encourage individuals to raise their concerns directly with our Data Protection Officer. We aim to resolve complaints promptly and

transparently.

14. Review

14.1. This Policy is controlled by and reviewed biennially by the organisation's Data Protection Officer (see paragraph 4.3 above for contact details).

14.2. When this policy is updated, changes will be published to our website.