Data Protection Policy

Play North West CIC (trading as Play Northwest)
Company No.: 15796794
Policy version: 1.0
Adopted: 2026-10-25, by both directors
Review date: 2027-10-25 (annual review)
Data controller: Play North West CIC, 9 Old Lane, Eccleston Park, Prescot, L34 2RE
Data protection lead: John Paul Randles, Director
Deputy: Andrew Reeves, andrew@playnorthwestcic.com
Contact: hello@playnorthwestcic.com · 07808 238730

1. Purpose

This policy sets out how everyone working for Play North West CIC must collect, use, store and share personal data.

Our participants often share sensitive information with us, including about their mental health, SEND or personal circumstances. They trust us with it. Handling it carefully is part of keeping them safe.

This is an internal policy for directors, facilitators and volunteers. It sits behind our public Privacy Policy, which tells participants and website visitors what we collect and what their rights are. This policy explains how we make sure those promises are kept.

2. The law and our principles

We follow the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. We apply the seven data protection principles. Personal data must be:

1. **Lawful, fair and transparent:** we have a lawful basis and tell people what we do with their data.
2. **Purpose limited:** used only for the reason we collected it.
3. **Minimised:** we collect only what we need to deliver sessions safely.
4. **Accurate:** kept up to date and corrected when wrong.
5. **Storage limited:** kept no longer than necessary.
6. **Secure:** protected against loss, theft and unauthorised access.
7. **Accountable:** we can show how we comply.

3. Roles and responsibilities

Who	Responsible for
Board of Directors	Overall accountability as data controller. Approves this policy and reviews it yearly.
Data protection lead (John Paul Randles)	Day-to-day compliance, the ICO registration, rights requests, breach handling, and keeping the record of data we hold.
Deputy (Andrew Reeves)	Covers the data protection lead when unavailable.
Facilitators, freelancers and volunteers	Following this policy, collecting only what is needed, keeping data secure, and reporting any breach immediately.

4. What we hold and why

Data	Whose	Lawful basis
Name and contact details	Participants, parents and carers, referrers	Consent, or legitimate interests in delivering sessions
Referral information (reason for referral, support needs)	Participants	Consent, given by the participant or with their agreement
Emergency contacts, parental consent for under-18s	Participants	Legitimate interests; legal obligation for safeguarding
Health, disability, SEND and access needs	Participants	Explicit consent (special category data)
Wellbeing scores and session feedback	Participants	Consent
Equality monitoring answers	Participants	Explicit consent; always optional
Safeguarding records	Participants	Legal obligation; substantial public interest (safeguarding)
Payment and donation records	Payers and donors	Contract; legal obligation (accounts)
DBS details, contracts, bank details for pay	Staff, freelancers, volunteers	Contract; legal obligation

Special category data (health, disability, ethnicity, religion, sexual orientation) needs extra care. We collect it only when it helps us support someone safely or monitor equality. We ask for explicit consent, explain why, and never make it a condition of taking part except where needed for safety.

The data protection lead keeps this table up to date as our record of processing.

5. Keeping data secure

Digital

- Store participant data only in Play North West CIC accounts, never in personal email, personal cloud storage or personal messaging apps.
- Protect all devices with a password, PIN or biometric lock, and keep software up to date.
- Use strong, unique passwords and two-factor authentication on email and cloud accounts.
- Limit access to people who need it for their role.
- Send sensitive information by password-protected file or secure link, not in the body of an email.

Paper

- Keep paper forms (registers, consent forms, feedback forms) in a closed folder during sessions and never leave them unattended.
- Transfer them to secure digital storage within 7 days, then shred the paper, or store it in a locked cabinet.

In sessions

- Do not discuss a participant's personal details in front of others.
- Only take photos or recordings of participants with recorded consent (see section 9).
- Do not share participants' contact details with other participants.

6. How long we keep data

These periods match our public Privacy Policy.

Data	Kept for
Enquiry and booking data	Up to 24 months after last contact
Programme participation and wellbeing data	Up to 6 years for funder reporting, then anonymised or deleted
Payment and financial records	6 years (accounting requirements)
Safeguarding records	As set out in the Safeguarding Policy (typically 7 years for adults; longer for children)
Staff, freelancer and volunteer records	6 years after the working relationship ends
Website visit logs	30 days

The data protection lead checks stored data once a year and securely deletes anything past its retention date. Paper is shredded. Digital files are permanently deleted, including from shared folders and bins. Anonymous totals may be kept for reporting.

7. Requests from individuals

People have the right to access, correct, delete, restrict or move their data, to object to how we use it, and to withdraw consent at any time.

1. Anyone who receives a request, in any form, passes it to the data protection lead the same day.
2. The data protection lead confirms the person's identity, and for a child, whether they or a parent should make the request.
3. We respond within one calendar month, free of charge.
4. Where we cannot fully meet a request (for example, safeguarding records we must keep), we explain why and tell the person they can complain to the ICO.
5. Each request and our response is logged.

8. Data breaches

A data breach is any loss, theft, wrong disclosure or unauthorised access to personal data. Examples: a lost register, an email sent to the wrong person, a stolen laptop, or a hacked account.

1. **Report it immediately.** Tell the data protection lead straight away, even if you are unsure. Nobody will be blamed for reporting honestly.
2. **Contain it.** Recover the data if possible, change passwords, or ask a wrong recipient to delete an email.
3. **Assess the risk.** The data protection lead decides how likely and serious the harm to people is.
4. **Report to the ICO within 72 hours** of becoming aware, if there is a risk to people's rights. Use the ICO breach reporting service.
5. **Tell the people affected** without delay if the risk to them is high.
6. **Record and learn.** Log every breach, including ones not reported to the ICO, and the steps taken to stop it happening again.

If a breach puts someone at risk of harm, follow the Safeguarding Policy as well.

9. Sharing, suppliers, photos and apps

Suppliers (processors). We only use suppliers who protect data to UK GDPR standards, under a written agreement. Current suppliers are Stripe (payments), our email host, and Amazon Web Services (website hosting and online form data, stored in the United States). New suppliers are approved by the data protection lead and added to our Data Processing Agreement schedule.

Sharing with others. We never sell data or share it for marketing. We share personal data with referrers or partners only with the person's consent. We share with statutory services (MASH, police, LADO) without consent only where the law or safeguarding requires it.

Funders. We share only anonymous, combined figures, unless someone has given written consent for a named story or testimonial.

Photos, video and recordings. We get written consent before using anyone's image, voice or music publicly, and parental consent for under-18s. People can withdraw consent at any time, and we will stop future use.

Our apps. Connect & Support UK and WorkPathway UK follow the same rules. Wellbeing and journal data is stored on the user's device by default, and we collect only what is needed to run Premium features.

10. Training, related policies and review

Everyone who handles personal data reads this policy before they start and confirms they understand it. The data protection lead refreshes everyone's awareness each year.

This policy works alongside our Privacy Policy, Safeguarding Policy, Equality, Diversity & Inclusion Policy, Data Processing Agreement and Complaints Policy.

It is reviewed every year, or sooner if the law, our suppliers or our work changes.

Adopted by the directors of Play North West CIC on 25 October 2026: John Paul Randles (Director) and Andrew Reeves (Director).