Data Protection Policy

Internal governance for personal information used across counselling, assessment, training, supervision and commissioned services

Organisation	Moment of Truth Well-being Group Ltd
Document owner	Sharon Boyd, Director and Data Protection Lead
Version and status	Version 1.0 Apporved
Effective and review dates	Effective: 01/09/26 Review: September 2027
Complete before issue	[INSERT ICO REGISTRATION NUMBER] [CONFIRM PRIVACY EMAIL] [CONFIRM REGISTERED OFFICE]

Purpose and scope

Moment of Truth Well-being Group Ltd uses personal information to provide well-being and mental health services safely and effectively. This policy explains how the organisation meets its responsibilities as a controller and, where a contract requires it, as a processor. It applies to directors, employees, associates, trainees, volunteers and contractors.

This policy covers client and clinical records, enquiries, children and family information, workforce records, supplier information, recordings, photographs, outcome measures, assessment information and data handled for schools or commissioners.

Policy statement

The organisation will process personal information lawfully, fairly and transparently. It will collect information for clear purposes, limit collection to what is necessary, keep information accurate, retain it only as long as justified, protect it appropriately and remain accountable for its decisions.

Roles and accountability

Role	Responsibility
Directors	Approve policy, provide resources and oversee significant risks.
Data Protection Lead	Maintains the record of processing activities, advises on lawful bases, coordinates rights requests, complaints, breaches and impact assessments.
Clinical Lead	Ensures clinical records, confidentiality decisions, safeguarding disclosures and supervision arrangements meet professional standards.

Role	Responsibility
Managers	Control access, brief staff, check compliance and escalate concerns.
All workers	Use only authorised systems, follow minimum-necessary access, keep accurate records and report incidents immediately.
Processors	Act only on documented instructions under a compliant written contract.

The organisation will formally assess whether it must appoint a statutory Data Protection Officer. Until then, the Data Protection Lead coordinates compliance without implying that the role is a statutory DPO appointment.

Lawful processing

Before processing starts, the organisation will identify and record an Article 6 lawful basis. For special category information, including health information, it will also identify an Article 9 condition and any relevant Data Protection Act 2018 Schedule 1 condition. Consent will only be used when it is freely given, specific, informed, unambiguous and genuinely withdrawable.

- Service delivery may rely on contract, steps requested before a contract, legitimate interests, legal obligation or vital interests, depending on the circumstances.
- Clinical and safeguarding information requires a documented special category condition. The organisation will not assume that consent is the only or always the most appropriate condition.
- Criminal offence data will only be processed with official authority or an applicable Schedule 1 condition and safeguards.
- Where Schedule 1 requires an Appropriate Policy Document, the Data Protection Lead will maintain one alongside the record of processing activities.

Children and young people

Children have their own data protection rights. Capacity, maturity, best interests, confidentiality, parental responsibility and safeguarding will be considered case by case. No fixed age will automatically determine whether a parent can access a child's counselling record.

- Give privacy information in language the child or young person can understand and provide an adult version for parents or carers where appropriate.
- Build higher protection into services, forms, systems and online features likely to be used by children.
- Collect the minimum information required and avoid routine marketing or profiling of children.
- Record the rationale for disclosures to parents, schools, commissioners or safeguarding agencies.

Data protection by design and impact assessments

New systems, assessments, monitoring, AI tools, recordings, large-scale special category processing, data sharing arrangements and online services for children must undergo early privacy screening. A formal Data Protection Impact Assessment is required where processing is likely to create a high risk to people.

Individual rights and complaints

- Provide clear privacy information and routes to exercise rights.
- Recognise verbal and written rights requests and send them promptly to the Data Protection Lead.
- Respond within the applicable statutory period, normally one month, subject to lawful extensions, identity checks and exemptions.
- Operate a data protection complaints process, acknowledge complaints within the legal timeframe, investigate without undue delay and explain the outcome and the right to complain to the ICO.

Security and working practices

- Use organisation-approved accounts and systems, including Tacklit where authorised for clinical case management.
- Apply role-based access, multi-factor authentication where available, strong unique passwords, secure backups, patching and device encryption.
- Do not use personal email, unapproved messaging, personal cloud storage or removable media for client information unless specifically authorised and risk assessed.
- Verify recipients before sending, use secure transfer for sensitive information and share only what is necessary.
- Keep paper records locked, transport them only when necessary and never leave them unattended in vehicles or public places.
- Maintain confidentiality when working remotely, online, by telephone, in schools and in community settings.

Sharing and processors

Information may be shared where there is a lawful basis and the sharing is necessary and proportionate, including for safeguarding, serious risk, legal requirements, service delivery or a valid contract. The organisation will define controller and processor roles for each school or commissioner rather than assuming one status for every contract. Processor contracts must include the mandatory Article 28 terms.

Retention disposal and incidents

The Records Retention and Secure Disposal Policy governs retention. All suspected loss, unauthorised access, misdirection, disclosure or alteration must be reported immediately. The Data Protection Lead will record every breach, assess risk, notify the ICO within 72 hours where required and inform affected people without undue delay where the risk is high.

Training monitoring and review

Workers must complete data protection and information security training at induction and refresher training at least annually. The organisation will audit access, retention, processor contracts, privacy information, rights requests, incidents and action plans.

Legal and guidance sources

- UK General Data Protection Regulation, as amended
- Data Protection Act 2018, as amended by the Data Use and Access Act 2025
- Privacy and Electronic Communications Regulations 2003, as amended
- ICO guidance for organisations, including children and the UK GDPR, storage limitation, security, individual rights, direct marketing and personal data breaches

Source check completed September 2026. The organisation must review this document sooner if its services, systems, contracts or the law change.