Privacy Statement & Data Protection Policy

Statutory Information Governance, Online Form Security Architecture & UK GDPR Compliance (Policy 05 v3.2)

DisabilityPlus is dedicated to protecting client confidentiality, privacy rights, and personal data. This policy defines our statutory information governance protocols under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). It outlines how we process, store, and protect clinical and special category data, with specific emphasis on the end-to-end security architecture of online intake forms completed by clients.

1. Who we are and how to contact us

DisabilityPlus (DISABILITY+ LTD., Registered in England and Wales, Company number 13411626) [and, for our Deaf service users, our sister company Deaf4Deaf (DEAF4DEAF LIMITED, Company number 10070652), which operates under full DisabilityPlus governance] is committed to protecting your privacy, confidentiality, and personal data.

Under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), DISABILITY+ LTD. acts as the Data Controller for all personal and clinical information we hold about you.

Governance role or contact channel	Official details
Data Controller	DISABILITY+ LTD. (trading as DisabilityPlus), Company number 13411626
Registered office address	DisabilityPlus House, Pembroke Avenue, Hersham, Walton-On-Thames, Surrey, KT12 4NT
Responsible Data Protection Official	Simon Lloyd (Managing Director) - simon.lloyd@disabilityplus.co.uk
Client Services Manager	Annette - client.services@disabilityplus.co.uk
Telephone and text / WhatsApp	Office: 01932 881 849 (Mon-Fri, 9:30 am - 5:00 pm) / Text or WhatsApp: 07539 877 357
Website	https://www.disabilityplus.co.uk/

2. What information we collect about you and how we collect it

To provide you with safe, accessible, peer-matched psychological therapy from a registered Psychologist or Psychotherapist who shares lived experience of your condition, we only collect information that is necessary for your care, safety, and funding administration.

To avoid cognitive, sensory, or physical exhaustion, we collect your information in two simple stages:

- **Pre-assessment online intake:** Before your first session, we send you a secure digital intake form (which you can complete yourself or with the support of a parent, family member, or carer) covering your basic contact details, GP surgery details, emergency contact, personal goals for therapy, simplified safety and specific disability questions, and your signed digital consent.
- **Clinical consultation with your psychologist or psychotherapist:** During your assessment and ongoing therapy sessions, your assigned Psychologist or Psychotherapist records clinical notes and conducts any remaining mental health questionnaires conversationally at your pace.

Category of personal data	Examples of what we collect
Identity and contact details	Full name, date of birth, address, postcode, email address, telephone/mobile number, preferred pronouns, and communication or accessibility requirements (under the NHS Accessible Information Standard DCB1605).
Emergency and medical contacts	Name and contact details and address of your registered GP surgery.
Special category health and clinical data	Details of your physical, neurological, or sensory disability, medical history, current medications, mental health presentation, questionnaire scores, risk assessments, safety plans, and session notes recorded by your Psychologist or Psychotherapist.
Funding and billing administration	NHS Integrated Care Board (ICB) or Local Health Board commissioning references, Personal Health Budget (PHB) or Access to Work reference numbers, charity grant details (such as the Rosie Jones Foundation), or self-pay invoicing records.

3. Our lawful basis for processing your personal data

Under the UK GDPR and the Data Protection Act 2018, we must have a valid legal reason (lawful basis) to collect and use your information. Because we process health and clinical records ("Special Category Data"), we satisfy both Article 6 and Article 9 of the UK GDPR:

UK GDPR / DPA 2018 article	How this applies to your care at DisabilityPlus
Article 6(1)(a) and Article 9(2)(a) - Explicit consent	When you sign our Consent Form, you give explicit consent for us to hold your clinical records and, where requested by you, share your Mental Health Assessment, Treatment Plan, or Progress Report with your GP, NHS commissioners, or chosen funding body.
Article 6(1)(b) - Performance of a contract	Processing your contact, scheduling, and billing information so we can book your appointments, send appointment reminders, and administer your sessions.
Article 6(1)(e) and 6(1)(f) - Public interest and legitimate interests	Coordinating with NHS Integrated Care Boards (ICBs), GPs, and statutory bodies where your therapy is funded by the NHS, a Personal Health Budget (PHB), or a third-party grant.
Article 9(2)(h) and DPA 2018 Schedule 1, Part 1, Paragraph 2 - Health and social care	Processing special category health data for the provision of psychological health care and treatment by regulated health professionals (Psychologists and Psychotherapists registered with HCPC, BPS, UKCP, BACP, or NCPS) bound by a statutory duty of confidentiality.
Article 6(1)(d), Article 9(2)(c) and DPA 2018 Schedule 1, Part 2, Paragraph 18 - Vital interests and safeguarding	In rare emergencies where there is an immediate, serious risk to your life or physical safety, or a statutory safeguarding concern regarding a child or vulnerable adult, the law allows us to share necessary safety information with your GP or emergency services without delay.

4. How we store and protect your data (WriteUpp ISO/IEC 27001 security)

We do not keep paper clinical files. All of your personal and clinical records are stored inside WriteUpp (developed by Pathway Software Limited, ICO Registration No. Z2865352), a specialist clinical practice management and electronic health record (EHR) platform that has been a trusted supplier to NHS therapy services teams for over 10 years. WriteUpp acts as our Data Processor under UK GDPR Article 28.

- **ISO/IEC 27001 certification:** WriteUpp's systems and security processes are certified to the international ISO/IEC 27001 information governance standard (Certificate No. 275372022) and are audited annually.
- **Encryption and EU geo-replication:** Your data is encrypted both in transit (via 256-bit SSL encryption) and at rest. For business continuity and protection against data loss, encrypted records are geo-replicated across two separate EU-based data locations, each with four server clusters.
- **Mandatory two-factor authentication (2FA) and Caldicott protection:** Access to WriteUpp is restricted strictly to authorised DisabilityPlus staff and your assigned Psychologist or Psychotherapist using mandatory two-factor authentication (2FA). Every service user is assigned

an anonymised WriteUpp ID (WUID) to protect your identity in administrative logs in line with the NHS Caldicott Principles.

- **Secure video consultations:** All online video therapy sessions are delivered through integrated, peer-to-peer, 256-bit WebRTC-encrypted telehealth platform. Video sessions are never recorded and require no third-party software downloads.
- **Clinical note-taking and supervision:** Your Psychologist or Psychotherapist records clinical notes directly inside WriteUpp (which includes secure clinical template tools to assist accurate note-taking, locked with immutable timestamps under Regulation 17). To ensure the highest clinical quality, your practitioner discusses their clinical work in confidential clinical supervision using only your anonymised initials or WriteUpp ID.
- **Secure Client Portal and appointment reminders:** WriteUpp sends automated SMS or email appointment reminders (in line with the Privacy and Electronic Communications Regulations [PECR 2003]). Where magic links or the 24/7 Client Portal are used, identity verification requires your date of birth and postcode, and access is restricted strictly to that specific appointment.

4.1 Security Architecture of Online Client Forms & Digital Answers

A foundational commitment of our clinical governance is ensuring the comprehensive security and confidentiality of the answers clients submit via our online forms. Online intake questionnaires digital consent instruments, and 24/7 Client Portal interactions are managed under rigorous technical and operational controls:

- **256-Bit SSL/TLS Encryption in Transit:** All online intake forms operate over secure HTTPS channels protected by 256-bit SSL/TLS encryption. Client answers, medical history, and contact details are fully encrypted before leaving the client's browser, preventing interception, eavesdropping, or tampering during transmission across the internet.
- **Direct EHR Integration & Elimination of Email Vulnerabilities:** Upon submission, client answers flow directly via secure internal APIs into WriteUpp's electronic health record (EHR) platform, automatically attaching to the client's locked electronic chart. Responses are never routed through unencrypted email systems, nor are they temporarily cached in unsecured web hosting databases.
- **AES-256 Storage Encryption & Dual EU Geo-Replication:** Completed form answers and clinical records are stored using AES-256 encryption at rest on Microsoft Azure cloud infrastructure. Records are geo-replicated across two separate EU-based geographic data locations, spanning four isolated server clusters in each facility, ensuring continuous disaster recovery, business continuity, and data preservation.
- **Role-Based Access Control & Mandatory Two-Factor Authentication (2FA):** Access to completed online client forms is strictly restricted to authorised DisabilityPlus clinical governance staff and the client's assigned peer-matched practitioner. All clinical and administrative logins mandate Two-Factor Authentication (2FA), preventing unauthorised internal or external access.
- **Regulation 17 Audit Logs & Immutable Timestamp Locks:** In compliance with Regulation 17 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, all completed digital forms, consent records, and notes are locked with immutable timestamps and author locks. Submitted answers cannot be modified, overwritten, or backdated, preserving forensic data integrity.
- **NHS Caldicott Principles & Pseudonymous WriteUpp IDs (WUIDs):** Every client is allocated a unique WriteUpp ID (WUID). System logs, administrative registers, and technical maintenance

processes reference only this anonymised identifier, isolating identifiable personal answers from non-clinical operational staff.

- **Secure 24/7 Client Portal & Restricted Magic Links:** Where clients utilise our 24/7 online portal to manage appointments, access is protected by two-point identity verification requiring date of birth and postcode validation. Magic link invitations are tied exclusively to specific appointment records and expire automatically, preventing persistent URL reuse.

5. Confidentiality and when we share your information

Everything you discuss with your Psychologist or Psychotherapist is treated as strictly confidential. We never sell, rent, or trade your personal data to any third party.

We only share your information outside DisabilityPlus in the following specific circumstances:

- **With your explicit consent (for GP and NHS funding support):** Where you ask us to support you with an NHS funding request (such as a Direct to Mental Health Commissioners application or a Mental Health Assessment and Treatment Plan prepared for your GP to submit for a Mental Health Personal Health Budget [PHB]) or a charity grant (such as the Rosie Jones Foundation), we share the agreed assessment, treatment plan, and progress reports with your named GP surgery and the relevant NHS commissioning team.
- **Start-of-session safety check and our 24-hour welfare protocol (DAAP):** At the start of each remote session, your Psychologist or Psychotherapist confirms your physical location and contact details to keep you safe. Under our Disability-Adjusted Attendance Policy (DAAP), if you miss a scheduled session without letting us know, we will try to contact you within 24 hours to check you are safe and have not experienced a medical or communication crisis. If we cannot reach you or your emergency contact within 24 hours and have serious concerns for your welfare, our Designated Safeguarding Lead (Victoria Nelson) or Deputy Safeguarding Lead (Simon Lloyd) may contact your GP surgery or local welfare services.
- **Immediate risk of serious harm or statutory safeguarding:** If you disclose an immediate intention to seriously harm yourself or another person, or if a serious safeguarding concern arises under the Care Act 2014 or Children Act 1989, we have a legal and ethical duty to share only the minimum necessary information with your GP, local NHS Crisis Team, or safeguarding authorities. Wherever safe and possible, we will always discuss this with you first.
- **Legal obligation:** Where we are required to disclose information by a UK court order or statutory authority.

6. How long we keep your records (retention schedule)

In line with the NHS Records Management Code of Practice (2021), the Limitation Act 1980, and our clinical indemnity insurance requirements, we retain clinical records for the following periods after your therapy ends:

Type of record	Retention period after discharge
Adult psychological therapy and clinical health records	Retained securely for a minimum of 8 years after your final session (and up to 20 years for complex long-term mental health records in line with NHS Records Management Code of Practice 2021 guidelines), after which they are permanently and securely erased from WriteUpp.
Young people supported under our Exceptional Under-18 Peer-Matched Policy	Retained until the service user's 25th birthday (or 26th birthday if aged 17 when therapy ended), or 8 years after discharge, whichever is longer.
Financial and invoicing records	Retained for 6 years plus the current financial year to comply with HM Revenue and Customs (HMRC) and NHS audit regulations.

7. Your data protection rights under UK GDPR

Under the UK GDPR, you have clear legal rights over the personal information we hold about you, which are fully supported by WriteUpp's dedicated GDPR compliance tools:

- **The right to be informed (Articles 13 and 14):** The right to clear, accessible information about how we use your data (as set out in this Privacy Statement).
- **The right of access / Subject Access Requests (Article 15):** You have the right to request a copy of the personal and clinical records we hold about you free of charge. Once we verify your identity, we will provide your records within one calendar month.
- **The right to rectification (Article 16):** If any factual personal information we hold about you (such as your address, GP details, or medical history) is inaccurate or incomplete, you have the right to ask us to correct it.
- **The right to erasure / to be forgotten (Article 17):** You can ask us to delete your personal data where there is no compelling legal or clinical reason for us to continue holding it. Please note that while we can immediately delete marketing or enquiry data, UK healthcare law and clinical indemnity regulations require us to retain completed clinical health records for the statutory retention period set out in Section 6.
- **The right to restrict processing or object (Articles 18 and 21):** You can ask us to restrict how we use your data, and you can withdraw your consent for us to share reports with third parties at any time by emailing us.
- **The right to data portability (Article 20):** You have the right to receive the personal data you have provided to us in a structured, commonly used electronic format or ask us to transfer it securely to another healthcare provider.

To exercise any of these rights, please contact Simon Lloyd (Managing Director) at simon.lloyd@disabilityplus.co.uk or Annette (Client Services Manager) at client.services@disabilityplus.co.uk (or call 01932 881 849).

8. Questions, accessible formats, and how to raise a concern

In line with the NHS Accessible Information Standard (DCB1605), we are happy to provide this Privacy Statement in alternative accessible formats on request (including large print, screen-reader friendly plain text, Easy Read, or a British Sign Language [BSL] video explanation).

If you ever have any questions or concerns about how we handle your personal information, please contact Simon Lloyd at simon.lloyd@disabilityplus.co.uk in the first instance so we can resolve it promptly for you.

You also have the right to raise a concern directly with the UK's independent data protection regulator, the Information Commissioner's Office (ICO):

- Website: https://ico.org.uk/
- Telephone helpline: 0303 123 1113
- Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Executive Sign-Off & Data Controller Declaration:

Authorised Signatory	Simon Richard Lloyd Managing Director, Co-Founder, Deputy Designated Safeguarding Lead (DDSL), & Responsible Data Protection Official
Data Controller (Legal Entity)	DISABILITY+ LTD. (Company No. 13411626, trading as DisabilityPlus) Registered Office: DisabilityPlus House, 25 Pembroke Avenue, Hersham, Walton-On-Thames, Surrey, KT12 4NT
Official Direct Contact	Email: simon.lloyd@disabilityplus.co.uk | Office: 01932 881 849 | Text/WhatsApp: 07539 877 357
Policy Version & Governance Cycle	**Policy 05 (Version 3.1) | Annual Review Cycle | Next Formal Review Date: September 2027**
Executive Signature & Date	 *Simon Richard Lloyd, Managing Director* **Date: 17 September 2026**