DATA PROTECTION, CONFIDENTIALITY AND RECORDS MANAGEMENT POLICY

Clinical practice, supervision and business administration

Organisation	Norfolk Therapy Services / NorfolkCBT
Data controller	Norfolk Therapy Services / NorfolkCBT
Information governance lead	Russell Wharton
Contact	russell@norfolkcbt.co.uk | 07712 008245
Policy adopted	29 August 2026
Review date	By 29 August 2027, or sooner following a material change or incident
Key systems	WriteUpp; reMarkable for limited supervision use; locked paper storage

1. Purpose and policy statement

This policy explains how NorfolkCBT collects, uses, records, stores, shares, retains and securely disposes of personal information. It applies to client assessment and therapy, clinical supervision and consultation, enquiries, appointments, reports, billing, safeguarding, complaints, professional requirements and business administration.

NorfolkCBT recognises that clinical information is highly sensitive. It will process personal information lawfully, fairly, transparently and securely; collect only what is relevant; keep it accurate; retain it no longer than necessary; and respect the rights of individuals. Confidentiality is fundamental to therapeutic and supervisory relationships but is not absolute where disclosure is required or justified by law, safeguarding or prevention of serious harm.

2. Scope and accountability

Norfolk Therapy Services / NorfolkCBT determines the purposes and means of processing and is the data controller. Russell Wharton is responsible for information governance, responding to rights requests,

managing incidents, reviewing processors and contracts, maintaining the ICO registration/fee where required, and reviewing this policy.

WriteUpp acts as a data processor for patient data entered into the service. Other suppliers may act as processors or independent controllers depending on the service. Use of a reputable system does not transfer NorfolkCBT's responsibility for choosing appropriate settings, access controls, retention and disclosure decisions.

This policy applies to all formats and locations, including WriteUpp, reMarkable, computers and mobile devices, email and messaging, paper records, reports, downloaded files, backups under a processor's control, and information received from referrers or third parties.

3. Data protection principles

- Lawfulness, fairness and transparency: people are told how their information is used, subject to lawful exceptions.
- Purpose limitation: information is used only for specified, explicit and legitimate purposes, or a compatible lawful purpose.
- Data minimisation: only information reasonably necessary for care, supervision, safety, administration and accountability is recorded.
- Accuracy: reasonable steps are taken to distinguish fact, observation, third-party information and clinical opinion, and to correct material inaccuracies.
- Storage limitation: information is retained under the schedule in this policy and securely disposed of when no longer required.
- Integrity and confidentiality: proportionate technical and organisational safeguards protect against unauthorised access, loss, alteration or disclosure.
- Accountability: decisions, contracts, incidents, rights requests, retention and relevant risk assessments are documented.

4. Categories of information

- identity and contact details, date of birth, address, GP, emergency contacts and parental-responsibility information;
- health, mental-health, disability, neurodivergence, medication, risk, safeguarding and treatment information;
- appointment, communication, consent, clinical assessment, formulation, care plan, progress and outcome records;
- referral information, reports, correspondence and information from or shared with other professionals;
- payment, invoice and limited financial administration information;
- supervisee identity, contact details, professional role, supervision contract, attendance, development, practice issues and agreed actions;

- anonymised or pseudonymised material about clients discussed in supervision; and
- technical and audit information generated by practice systems.

Health information and some information about sex life, sexual orientation, race, ethnicity, religion or belief are special-category data and receive additional protection. Information about criminal allegations or offences is handled with particular care and only where lawful.

5. Purposes and lawful bases

5.1 Clinical services and supervision

Personal information is processed where necessary to take steps at a person's request before entering a contract and to perform the contract for assessment, therapy, supervision or consultation. Clinical health information is additionally processed under an appropriate UK GDPR Article 9 condition, normally provision of health care or treatment by a professional subject to confidentiality, and where relevant for safeguarding, legal claims, substantial public interest or vital interests. Explicit consent will be used where it is the most appropriate condition, but will not be presented as the sole basis for all necessary clinical record-keeping.

5.2 Legal, safeguarding and professional obligations

Information may be processed to comply with law, professional standards, court orders, regulatory requirements, insurance conditions, tax and accounting duties, or to establish, exercise or defend legal claims. Information may be shared without consent where necessary and proportionate to safeguard a child or adult at risk, prevent serious harm or crime, protect vital interests, or meet another legal duty. Decisions and rationale will be recorded.

5.3 Administration and legitimate interests

Legitimate interests may support proportionate processing for practice administration, service security, debt recovery, quality assurance, responding to enquiries and defending complaints, after balancing the individual's rights and expectations. Direct marketing will not use clinical information and will follow consent and electronic-marketing rules.

6. Transparency and consent

Clients and supervisees will receive an appropriate privacy notice explaining the controller's identity, purposes, lawful bases, categories, recipients, retention, international transfers where applicable, rights, complaint route and any consequences of not providing necessary information. Privacy information will be available before or when data is collected, with additional explanation where information is obtained from another source.

Clinical consent, contractual agreement and consent under data protection law are distinct. Consent must be specific, informed, freely given, unambiguous and recorded where relied upon, and can be withdrawn for future consent-based processing. Withdrawal does not require deletion of records that remain necessary under another lawful basis or for legal, professional or safety reasons.

7. Authoritative clinical record: WriteUpp

WriteUpp is the principal and authoritative record for client assessment, treatment, risk, safeguarding, correspondence, documents, appointments and relevant administrative activity. Material clinical decisions and information needed for continuity, accountability or safety must be entered promptly, accurately and contemporaneously.

- Each user must have an individual account; passwords must not be shared.
- Two-factor authentication must be enabled and recovery methods kept secure.
- Access is restricted to the minimum necessary for the person's role and removed promptly when no longer required.
- Devices used to access WriteUpp must use supported software, strong authentication, automatic locking and device encryption where available.
- Downloads and exports are avoided unless necessary. Any necessary local copy must be encrypted, access-controlled, logged where appropriate and deleted securely after use.
- Audit trails, access settings, data-processing terms, sub-processors and security information will be reviewed periodically and after material supplier changes.

WriteUpp states that patient data is encrypted in transit and at rest, offers two-factor authentication and audit/security controls, and is ISO 27001 certified. Its current terms identify NorfolkCBT as controller and WriteUpp as processor and describe international processing safeguards and retained technical backups. NorfolkCBT will not describe WriteUpp as making the practice "automatically GDPR compliant"; compliance depends on how the system is configured and used.

8. Limited use of reMarkable for clinical supervision

The reMarkable device will be used only for notes made while providing clinical supervision to other practitioners. It will not be used as the primary clinical record for NorfolkCBT therapy clients, for initial assessments, or to store identifiable client records.

8.1 Data minimisation and anonymisation

- Clients discussed in supervision must not be named. Do not record full initials, date of birth, address, telephone number, email, NHS number, employer, school, exact location or a distinctive combination of details that could reasonably identify them.
- Use a non-identifying case label where needed. Record only the minimum clinical detail necessary for supervision.
- The supervisee may be identifiable because the supervision record concerns their professional practice. It must therefore be treated as confidential personal data even where client material is anonymised.
- Safeguarding or other information requiring identifiable action must be recorded directly in the appropriate secure authoritative record, not left solely on the tablet.

8.2 Device and transfer controls

- Protect the device with a strong passcode and enable device encryption/data protection where the model supports it.
- Keep Wi-Fi switched off except for the shortest period necessary to complete an authorised transfer. Disable automatic or unnecessary integrations and do not use public Wi-Fi.
- Preferred practice is a direct USB transfer where practicable, using the reMarkable USB web interface, because this can avoid unnecessary cloud synchronisation.
- If Wi-Fi/cloud transfer is used, only the minimised supervision material described above may be transferred. The reMarkable account must use a unique strong password and multi-factor authentication where available, and current privacy, security and international-transfer terms must be reviewed.
- After confirming that the record has transferred accurately into WriteUpp, delete the source from the reMarkable immediately and empty any device trash or deleted-items area. Check that the item is no longer visible in connected apps or cloud storage.
- The tablet must not be left unattended in public or routinely stored in a vehicle. Loss, theft, unexpected synchronisation or misdirected sharing is treated as a potential data incident.

Deletion from a synced device may not mean immediate erasure from all provider backups. The practice therefore relies first on anonymisation, minimisation and short retention on the device, and will keep the supplier relationship and settings under review.

9. Paper notes

Paper may be used for limited contemporaneous or working notes. Paper notes must contain the minimum necessary information, be kept in a locked cabinet when not in active use, and never be left visible in shared or public areas. Transport outside the practice must be avoided; if essential, records must remain under the practitioner's control in a closed, secure container.

Material information needed for care, risk management, safeguarding, continuity, accountability or future reference must be transferred into WriteUpp promptly. At the end of treatment, supplementary paper working notes are cross-checked against the WriteUpp record and destroyed by cross-cut shredding or a confidential-waste service. This destruction applies to temporary paper notes, not to the authoritative WriteUpp clinical record retained under section 13.

10. Email, telephone, messaging and online work

- Use practice contact channels and verify recipient details before sending information. Use the minimum necessary content in email subject lines and messages.
- Sensitive reports or records should be sent through a suitably secure method, with password protection or separate-channel password exchange where proportionate.
- Autofill recipients and attachments must be checked before sending. Misdirected communications are treated as incidents.

- Voicemail and text messages should disclose minimal information unless the person has agreed a safe communication arrangement.
- Video sessions must be conducted privately using approved systems and headphones where appropriate. Sessions are not recorded unless separately justified, expressly agreed and covered by clear retention and security arrangements.
- Clinical information received through WhatsApp or similar channels must be minimised, transferred into WriteUpp if relevant to the clinical record, and deleted from the messaging channel when no longer necessary, subject to the limitations of recipient devices and backups.

11. Sharing and disclosure

Information is shared only where there is a lawful basis, an appropriate special-category condition where required, and a clear purpose. Wherever safe and practicable, the person will be told what will be shared, with whom and why. Consent will normally be sought for routine liaison, reports and referrals.

Information may be shared without consent where necessary and proportionate for safeguarding, serious risk, prevention or detection of crime, a court order or statutory requirement, professional or regulatory reporting, legal claims or vital interests. The practice will share the minimum necessary, use secure means, distinguish fact from opinion, and record the recipient, purpose, lawful rationale, information disclosed and whether the person was informed.

Supervision does not justify unnecessary identification. Case material discussed for supervision will be anonymised or robustly pseudonymised unless identification is necessary for safeguarding or another lawful purpose and the disclosure is proportionate.

12. Individual rights

Subject to legal exemptions, individuals may have rights to be informed; access their data; correct inaccurate data; erase data; restrict processing; object to certain processing; receive portable data; and receive safeguards around solely automated decisions. NorfolkCBT does not use solely automated decision-making to determine clinical care.

1. Record the request immediately and verify identity proportionately.
2. Clarify scope where this will assist without delaying the response.
3. Search all relevant systems and formats, including WriteUpp, correspondence, reports, paper and any temporary device records.
4. Review third-party information, confidentiality, safeguarding, legal privilege and applicable exemptions before disclosure.
5. Respond securely and normally within one month. Record the response and reasons for any lawful refusal, restriction or extension.

A request for erasure does not create an automatic right to delete a clinical record. Records may be retained where necessary for health-care purposes, legal obligations, safeguarding, public interest or legal claims. The individual will be told the outcome and may complain to the ICO.

13. Retention and secure disposal

Retention begins when the relevant episode or relationship ends, unless another event restarts the period. The schedule is reviewed against current professional-body, insurer, contractual and legal requirements. A legal hold, safeguarding need, complaint, claim or investigation overrides routine destruction until resolved.

Record	Default retention	Disposal / note
Adult clinical record in WriteUpp	7 years after treatment ends	Review before deletion; retain longer where required by insurer, law, claim, safeguarding or clinical justification.
Client under 18 at end of treatment	Until 25th birthday, or longer if required	Review against current insurer/professional guidance and any safeguarding or legal need.
Supervision contract and authoritative supervision record	7 years after supervision ends	Includes attendance, themes, agreed actions and professional/accountability matters; client material should remain anonymised.
Paper working notes	End of treatment, after reconciliation	Cross-cut shred or confidential waste. Do not destroy information absent from the authoritative record if it remains necessary.
reMarkable source notes	Immediately after verified transfer	Delete from device, trash and connected apps/cloud so far as controllable.
Enquiries not proceeding to treatment	12 months after last contact	Retain less where no continuing purpose; securely delete.
Invoices and accounting records	At least 6 years after relevant financial year	Retain to meet tax/accounting requirements; minimise clinical detail.
Complaints, incidents and legal claims	7 years after closure or longer if advised	Preserve while litigation, regulatory, insurer or safeguarding action is possible or active.

Secure disposal includes verified deletion from active systems, secure erasure of local files where reasonably possible, cross-cut shredding or accredited confidential waste, and deletion of unnecessary email or messaging copies. Processor-controlled backups may expire on the processor's documented cycle rather than instantly; access must remain restricted during that period.

14. Security controls and access

- Use unique strong passwords stored in a reputable password manager; enable two-factor authentication wherever available.
- Keep operating systems, browsers, apps, antivirus/security tools and device firmware supported and updated.
- Enable full-disk encryption, automatic screen lock, remote locate/wipe where appropriate and encrypted backups for devices handling practice data.
- Do not use shared accounts. Apply least-privilege access and review access periodically.

- Do not store sensitive information in unencrypted downloads, desktop folders, screenshots, personal notes apps or removable media.
- Use a private network or trusted encrypted connection; avoid accessing clinical systems on public/shared computers.
- Maintain business-continuity arrangements for loss of access to WriteUpp without creating uncontrolled duplicate records.
- Review processors before use, including contract terms, data locations, sub-processors, security, breach notification, deletion and international-transfer safeguards. Complete a DPIA where processing is likely to create high risk.

15. Personal data breach and incident response

A personal data breach includes loss, theft, unauthorised access, accidental disclosure, alteration, destruction or unavailability. Examples include a lost device or paper file, email sent to the wrong person, compromised password, unexpected cloud synchronisation, unauthorised WriteUpp access, ransomware or inability to access records needed for safe care.

6. Contain the incident immediately: recover or remotely secure devices, revoke sessions, change credentials, contact unintended recipients, isolate affected systems and preserve evidence.
7. Start an incident log and identify what happened, when it was discovered, data and people affected, likely consequences, containment and outstanding risk.
8. Notify relevant processor support and the cyber insurer where appropriate, without putting identifiable patient data into ordinary support messages unless a secure authorised route is provided.
9. Assess risk to people's rights and freedoms. If reportable, notify the ICO without undue delay and within 72 hours of awareness, even if information must initially be provided in phases.
10. Where the breach is likely to result in high risk, inform affected people without undue delay unless a lawful exception applies. Provide clear protective advice.
11. Document the decision whether or not to notify, complete remedial action and update systems, training, risk assessment or policy.

Clinical safety and safeguarding action must run alongside data-breach management where the incident creates risk of harm.

16. Children, capacity and representatives

Privacy information will be explained in accessible, age-appropriate language. The child or young person's competence, understanding, confidentiality and best interests will be considered separately from parental responsibility. A parent does not automatically have unrestricted access to all therapy information. Requests by parents, attorneys, deputies or representatives require verification of authority and consideration of the individual's rights, capacity, confidentiality, safeguarding and third-party information.

17. Governance, audit and review

- Maintain the ICO data protection fee/registration where required; current ICO guidance states that counsellors holding personal information electronically are generally required to pay the fee.
- Maintain an up-to-date privacy notice, data map/record of processing, processor list, retention schedule, breach log and relevant legitimate-interest or DPIA records.
- Review WriteUpp account access, two-factor authentication, exports, integrations, processor terms and sub-processors at least annually.
- Review reMarkable settings, encryption, passcode, connected apps, cloud account and transfer process at least annually and after firmware, account or service changes.
- Review this policy after any incident, complaint, rights request, new technology, new processing purpose, professional-guidance change or material supplier change.

Appendix A - Practical record workflow

- Record authoritative assessment, therapy, risk, safeguarding and supervision information in WriteUpp.
- If temporary paper or reMarkable notes are used, minimise identifiers from the outset.
- Transfer material information promptly and accurately into WriteUpp; distinguish clinical record from informal prompts.
- Verify the WriteUpp entry is complete and accessible before destroying or deleting the source.
- At end of treatment, reconcile and cross-cut shred paper working notes. Retain the WriteUpp record under the schedule.
- After each reMarkable transfer, delete the source immediately and check device trash and connected services.
- Log and assess any loss, misdirection, unexpected synchronisation or unauthorised access immediately.

Appendix B - Key sources

- **Information Commissioner's Office - data protection guidance:** https://ico.org.uk/for-organisations/
- **ICO - health and social care data protection fee guidance:** https://ico.org.uk/for-organisations/data-protection-fee/paying-a-data-protection-fee-what-do-you-need-to-know/human-health-and-social-care/
- **ICO - responding to a personal data breach:** https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/
- **WriteUpp - security:** https://www.writeupp.com/security
- **WriteUpp - Terms of Service / processor provisions:** https://www.writeupp.com/terms-of-service
- **reMarkable - data security:** https://support.remarkable.com/s/article/Data-security

- **reMarkable - USB import and export:** https://support.remarkable.com/s/article/importing-and-exporting-files