INFORMATION SECURITY POLICY

Localscript — transcription and anonymisation services

Last updated: 20 August 2026
Review date: 20 August 2027

---

1. PURPOSE AND SCOPE

This policy sets out how Localscript Ltd protects the information it holds — client recordings and transcripts above all, and the business records that come with running the service.

It is the policy referred to at **Annex D, paragraph 10** of the Localscript Data Processing Agreement, and at **section 8** of the Localscript Privacy Policy. It is provided to clients on request and may be attached to a Data Processing Agreement where a procurement process requires it.

It covers every device, account and process used to deliver the Services. It applies to one person, because one person delivers the Services.

Owner: Montagu Franks, Director. There is no security committee and no delegation. If something in this policy is not being followed, it is my responsibility and mine alone.

A note on scope. Every control in this document is one I actually apply. Sections that would be irrelevant to a one-person business — visitor passes, reception sign-in, server rooms, staff disciplinary procedures — are not included rather than included and marked not applicable.

---

2. THE THREAT MODEL I AM DEFENDING AGAINST

Security policies are more useful when they say what they are protecting against. Mine are, in order of realistic likelihood:

1. **Loss or theft of the processing machine** — the most probable incident by a wide margin.
2. **Compromise of an email or cloud account** through credential theft or phishing.
3. **Accidental disclosure** — a transcript sent to the wrong recipient, or a file left where it should not be.
4. **Silent third-party exposure** — data reaching a service I did not intend it to reach, through a synced folder, an automated tool, or a software dependency.

5. **Loss of availability** — hardware failure, or my own incapacity, leaving a client without their data.

Every control below maps to at least one of these. Controls that do not defend against a real risk are not included, because a policy nobody follows protects nobody.

I do not claim that all security incidents are preventable. Some are not, which is why sections 12 and 13 exist.

---

3. THE CORE ARCHITECTURAL CONTROL

The single most important security property of this service is structural rather than procedural:

Client recordings and transcripts are processed and stored on one machine, in the United Kingdom, and are not transmitted to any external service at any stage.

Speech recognition, speaker segmentation and identifying-detail detection all run on models installed and executed locally. No audio, transcript or metadata is sent to any external application programming interface, cloud service or third-party provider.

This is not a preference that could be quietly reversed for convenience. It is a contractual commitment in **clause 3.2(g)** and **Annex C** of every Data Processing Agreement I sign. Changing it would require the written agreement of every affected client.

Consequence I accept: this constrains what tooling I can use and what hardware I need. That constraint is the product.

---

4. DEVICE SECURITY

Control	**Implementation**
Processing machine	A single device, owned and controlled by Localscript Ltd, physically located in the United Kingdom
Encryption at rest	Full-disk encryption enabled on every device, verified after any operating system upgrade
Encryption recovery	The disk encryption recovery key is held securely and separately from the device, so

Control	Implementation
	that encrypted data can still be recovered if the device fails. It is not stored on the device, in email, or in any third-party cloud
Authentication	Device password plus biometric unlock; automatic lock after a short idle period
Operating system updates	Security updates applied within 14 days of release; critical patches, and updates addressing actively exploited vulnerabilities, within 72 hours. Automatic download is enabled and installation is scheduled between processing runs
Supported versions only	The device runs a version of the operating system for which security updates are still published
Malware protection	The operating system's built-in protections — Gatekeeper, notarisation checks and XProtect malware definitions — are enabled and left enabled, with automatic definition updates
Firewall	Enabled, inbound connections blocked by default
Sole use	No other person uses the processing machine. No guest accounts. No shared logins
Cloud sync	Working directories holding client data are excluded from all cloud synchronisation. Verified whenever the operating system is upgraded or reinstalled, as OS updates have been known to re-enable desktop and documents sync by default
Removable media	Client data on removable media is encrypted. Media is not used for transport unless a client specifically requires it

5. PHYSICAL SECURITY AND WORKING ENVIRONMENT

Localscript operates from a private residence. That is stated openly because it changes which physical controls are relevant.

- **Screen privacy.** The screen locks automatically after a short idle period and is locked manually whenever I leave the room. Transcripts and audio are not left open on an unattended screen.
- **Household.** No member of the household has access to the processing machine, its login, or any account holding client data. Client work is not discussed in detail with anyone.
- **Paper.** Client material is not printed. Where a note is made on paper it carries no participant name or identifying detail, and is destroyed once no longer needed.
- **Devices at rest.** The processing machine is not left unattended in a vehicle, a public place, or any shared or unsecured space. Encrypted backup media is stored securely and separately from the machine.
- **Working location.** Client recordings and transcripts are processed only at the registered premises, never in cafés, co-working spaces, libraries or in transit.
- **Networks.** Client data is never transferred over public or untrusted wireless networks. The working network is private, with a changed default administrator password and current firmware.
- **Power.** The processing machine is a laptop with an internal battery, so a domestic power interruption does not terminate a processing run or corrupt working files.

---

6. ACCOUNT AND ACCESS SECURITY

- **Multi-factor authentication** is enabled on email, domain registration, hosting, banking, accounting and every account that could be used to reach client information.
- **Unique, long passwords** for every service, generated and held in a password manager. No password is reused, and none is written down.
- **No forced rotation.** Passwords are changed when there is reason to believe one is compromised, not on an arbitrary schedule — in line with current National Cyber Security Centre guidance, which advises against routine expiry because it drives users towards weaker, predictable passwords.
- **No shared accounts.** No account credentials are given to any other person.
- **Access is limited to the named individual** identified at clause 3.3 of the Data Processing Agreement. Nobody else has, or is given, access to client recordings, transcripts, anonymisation logs or re-identification keys.
- **Account inventory.** A written list of every service holding business or client information is maintained and reviewed annually. Unused accounts are closed rather than left dormant.

- **Recovery routes** — recovery email addresses and phone numbers — are reviewed at the same time, because an account is only as secure as the weakest way back into it.
- **Phishing.** Unexpected attachments and links are treated as hostile, particularly those appearing to come from a client, a university, or a hosting or domain provider. Where a message is unexpected, I verify through a channel I already hold rather than by replying.

---

7. SOFTWARE AND DEPENDENCIES

The pipeline is built from open-source components, which makes software provenance a live risk rather than a theoretical one.

- **Provenance.** Software is installed only from the official distribution channel for that project — the recognised package index, the project's own repository, or the vendor. Not from search results, forum links or mirrors.
- **Dependency review.** Before a new library or model is added to the pipeline I check what it is, who maintains it, and whether it is actively maintained. Dependency versions are pinned so that an upgrade is a deliberate act rather than a side effect.
- **The network-call test.** Before any new tool, library, model or service is introduced, I establish whether it makes any outbound network connection during processing. **Anything that does is not used on client data.** This check happens before adoption, not after.
- **Licensing.** All software carries a valid licence covering the use made of it. No unlicensed or cracked software is installed on any device used for the Services.
- **No unnecessary software.** Software that is not needed to deliver the Services is not installed on the processing machine.
- **Configuration under version control.** Pipeline code and configuration are held in version control, so the exact state of the processing environment is recorded and any change is traceable and reversible.

---

8. TRANSFER OF CLIENT DATA

Recordings reach me by a route **the client chooses**, ordinarily the institutional secure file transfer service they are already approved to use. I do not introduce a transfer mechanism, and I do not operate an upload portal.

Recordings and transcripts are never sent as email attachments, and never through consumer file-sharing services. This is absolute.

Where a client has no suitable transfer service, an encrypted route is agreed in writing before any personal data moves, and I identify every third party involved in that route so the client can assess it themselves.

Deliverables are returned by the same route, or another the client specifies in writing.

Why the client chooses: the transfer route is the only point in the chain where a third party could touch the data, so the decision belongs to the controller who is accountable for it — not to me.

---

9. STORAGE, SEPARATION AND BACKUP

- Client recordings and transcripts are held in a defined working directory, separate from business records.
- The **re-identification key is held separately** from the transcripts it relates to, and is delivered to the client with the Deliverables.
- **Backups are taken daily** while any client work is in progress.
- Backups are **encrypted** and held on **removable media within the United Kingdom**. Backups are **not** held in any third-party cloud service.
- Backup media is stored securely and separately from the processing machine, so that one theft or one fire does not take both.
- **Backups are tested.** A restore is tested at least monthly, and after any change to the backup arrangement. An untested backup is not a backup.
- Backups are subject to the same **30-day deletion schedule** as live data. A deletion that leaves a copy in a backup is not a deletion, so backup retention is deliberately short — 30 days, not the twelve months a general-purpose business would keep.

---

10. RETENTION AND DELETION

Recordings, transcripts, anonymisation logs and re-identification keys are securely and permanently deleted **within 30 days of delivery**, including from backups, or earlier at the client's written request.

Written confirmation of deletion is provided on request.

Full detail sits in the Localscript Retention and Deletion Policy. Where that policy and the signed Data Processing Agreement differ, the Agreement prevails.

---

11. AUTOMATED TOOLING AND MODELS

- All models used in processing are **installed and executed locally**. None makes a network call in the course of processing client data.
- **No client data is used to train, fine-tune, evaluate or improve any model**, mine or anyone else's — nor for research, benchmarking, marketing or portfolio purposes. This is clause 3.2(o) of the Data Processing Agreement.
- Automated output is never delivered unreviewed. Every transcript is checked in full against the audio by the named individual, who corrects speaker attribution and confirms or amends every identifying detail flagged for pseudonymisation before delivery.
- No decision affecting any individual is made by automated means. The output is a document, reviewed by a person, returned to the researcher who commissioned it.

---

12. INCIDENT RESPONSE

A security incident is any event where client data may have been lost, disclosed, altered, corrupted or accessed without authorisation — including a lost device, a suspected account compromise, or a transcript sent to the wrong recipient.

On discovering an incident:

1. **Contain it** — disconnect the affected device or account, revoke sessions, change credentials.
2. **Establish scope** — which clients, which recordings, what data, over what period.
3. **Notify the affected client within 24 hours** of becoming aware, to the address in their Data Processing Agreement. This is a contractual commitment at clause 3.2(e), and it stands whether or not the incident is ultimately reportable.
4. **Support the client's own obligations** — they are the controller and decide whether to notify the Information Commissioner's Office and the data subjects. I provide whatever they need to make and act on that decision.
5. **Record it** — what happened, when, what was affected, what was done, what changed as a result. This record is kept whether or not the incident was reportable.
6. **Consider ICO notification in my own right**, where the incident affects my own controller-side data.

Notification is not conditional on the incident being my fault, or on being certain of its scope. A client told late has lost the time they needed. Where scope is still unclear at 24 hours, I notify with what is known and follow up.

---

13. CONTINUITY AND RECOVERY

Localscript is operated by one person. That is a genuine single point of failure and is not disguised here.

Hardware failure or theft. Two separate commitments, because they answer different questions:

	Target
Returning a client's data to them from encrypted backup, using a replacement device meeting section 4	**1 working day**
Restoring full processing capability on replacement hardware — operating system, pipeline, model weights, configuration	**5 working days**

The second figure is longer because model weights and dependencies have to be re-downloaded and the environment rebuilt. Where a deadline cannot survive that, I say so and release the client rather than hold the work.

Capacity. Where I cannot complete work in a timescale the client can accept, I say so promptly and release them to go elsewhere rather than hold the work.

Incapacity. Where I become unable to perform the Services through illness, incapacity or death, the client is notified as soon as reasonably practicable and chooses whether their data is returned or securely destroyed. **No other person is given access to client data in order to complete the work** without the client's prior written authorisation. This is clause 3.4 of the Data Processing Agreement. Standing written instructions sufficient to give effect to that clause are maintained and kept accessible.

Full detail sits in the Localscript Business Continuity Policy.

---

14. STAYING CURRENT

A one-person business has no security team, so keeping informed is a named task rather than something that happens by itself.

- I subscribe to National Cyber Security Centre advisories and to the security announcement channels of the operating system and the principal software components in the pipeline.

- Vulnerability notices affecting anything in use are assessed on receipt, and the patching timescales in section 4 applied.
- Actions taken in response are recorded, so that the reason for a change is retrievable later.

---

15. WHAT I DO NOT HOLD

Stated plainly, because a security policy that implies certification it does not have is worse than no policy:

- Localscript Ltd does **not** hold ISO 27001, Cyber Essentials or Cyber Essentials Plus certification.
- There is no external audit of these controls, and no independently certified information security management system.
- Professional indemnity and cyber liability insurance is in place from the commencement of the first paid engagement, not before.

Where a client's procurement process requires certification I do not hold, I will say so at the point of enquiry rather than after a contract is signed.

---

16. REVIEW

This policy is reviewed annually, and additionally whenever:

- the processing pipeline changes materially;
- a new tool, library or service is introduced;
- an incident occurs;
- a client identifies a gap.

The review date is recorded at the top of this document.

Localscript Ltd is registered in England and Wales, company no. 17388152 · registered office 13 The Terrace, Barnes, London, SW13 0NP · registered with the Information Commissioner's Office, reference ZC217301 · monty@localscript.co.uk