

Privacy concept

Local school version

Processing, protection and rights

No stored audio recordings. No voice profiles.

Names from the class, private statements and off-topic remarks are filtered before the learning notes are filed. Review by teachers is optional.

All files and data of the local school installation are encrypted in storage and in transit. The school determines the retention period of learning content; the default is one school year.

This document describes the **local school version of ContextFriend**: processing, protective measures and rights. During setup at a school, every installation is checked against this concept and documented.

The responsible school adds its own contact details, legal bases, functions and deletion dates. This general product concept replaces neither its privacy notices nor a required data protection impact assessment or a contract for processing on behalf (Art. 28 GDPR).

In this full privacy concept

Responsibility and legal bases · Page 2

Processing and filtering · Page 4

Access and further protective measures · Page 6

Recipients and maintenance · Page 8

Version, evidence and sources · Page 10

Data categories and purposes · Page 3

Encryption · Page 5

Retention periods and deletion · Page 7

Rights and data protection incidents · Page 9

Summary version: separately on the privacy page

Provider and publisher

TamerinTECH GmbH

Seestr. 19

83727 Schliersee

Germany

Telephone: +49 8026 387 25 98

hello@context-friend.com

www.tamerin.tech

Managing director: Ron Tamerin

Responsible for content: Ron Tamerin

Address as shown

Register court: Amtsgericht München

Commercial register: HRB 263667

VAT ID: DE340834936

Privacy contact: hello@context-friend.com

[Full Impressum on the website](#)

Responsibility and lawfulness

1. Scope

The local school version serves the follow-up of specific teaching units. It creates subject-related learning notes, makes lawfully provided materials accessible and, where permitted by the school, allows questions to a local AI. Speech recognition, filtering, AI, search, account management and storage take place on the school server.

The requirements apply to all persons whose data is affected: students, teachers, school support assistants, substitute teachers and other persons present, as well as authorised parents and guardians. Mere website visits and contact forms are described separately in the [privacy policy of the public website](#).

2. Controller and data protection contacts

School: The controller within the meaning of the GDPR is the school or the body named in its school-specific notices. It decides on purpose, legal basis, scope, user group, retention periods and operation. The school management organises the approval; the school's data protection officer advises and monitors independently. The school's maintaining body (Schulaufwandsträger) and the school IT take on the operational tasks assigned to each of them.

Provider: TamerinTECH GmbH supplies the product. This supplier role alone does not confer access to lesson data. Where it is instructed to process personal data, for example in support, TamerinTECH acts only on instruction and on the basis of a required contract under Art. 28 GDPR.

Contact: The school publishes its address and the official contact of its data protection officer before use. Data protection enquiries to TamerinTECH reach the contact point at hello@context-friend.com or the provider address on page 1. A contact point is not automatically a formally designated data protection officer. Any required designation and publication of the officer's contact details take place separately under Art. 37 GDPR and § 38 BDSG (Federal Data Protection Act).

3. Legal bases and required information

For state schools in Bavaria, the provisions to be examined are in particular Art. 6(1)(e) and (3) GDPR, [Art. 85 BayEUG](#) (Bavarian Education Act) and [§ 46 BaySchO with Annex 1](#) (Bavarian School Regulations). They do not give blanket permission for continuous capture of lessons. Speech processing, learning storage, access and security logs must each be examined for necessity and suitable alternatives.

For voluntary functions, any required consent must be obtained in a specific, informed, freely given and future-revocable manner. The school clarifies the representation of minors, an equivalent alternative without disadvantage and the participation rights of employees. Signing in and reading this document do not replace consent.

Special categories of personal data, such as health information, are not deliberately collected. If their processing is unavoidable, Art. 9 GDPR must additionally be observed; if there is no sound basis, capture must be suspended. The right to one's own spoken word must also be respected.

Data categories and purposes

4. Which data is processed

Data category	Content, purpose and limit
Spoken language	Speech during expressly activated lesson segments for local conversion into text. Voices are never stored, archived or backed up as an audio file. No playback, no voice profile.
Unprocessed text	Recognised wording solely for local content filtering. Discarded after filtering, at the latest five minutes after capture. No permanent filing, no search source and no backup.
Learning notes and materials	Subject-related explanations, examples, tasks, source references and documents lawfully provided by the school. Purpose: follow-up and revision in the authorised course.
Search data and derivatives	Text passages, local search indexes, embeddings and subject-related links. They receive the same permissions and deletion dates as their sources.
Questions and answers	Your own entries, answers and conversation context for the respective learning question. A permanent history is kept only with the school's approval and is explained beforehand. No general access by other students.
Access and authorisations	Necessary identifiers, protected login data, roles, course assignments and required approvals. No public directory of persons; no precautionary collection of private profile details.
Security data	Required sign-in, access and administrative events, where applicable IP addresses and timestamps. Purpose: access protection and troubleshooting. No lesson texts, chat content or secret access values in logs.
Backup copies	Encrypted copies of the expressly permitted stored holdings for recovery. No audio or raw-text copies; limited access rights and duration.

4.1 Origin and personal reference

Data arises in the activated lesson segments, through your own entries, school course assignments and materials provided. For external data sources, the school provides the required information under Art. 14 GDPR. The mere possibility of processing data is not permission to collect all data categories.

Voice, question content, identifier or context can make a person identifiable. Name filters and pseudonyms are not complete proof of anonymity. The statement about removed names refers to the learning notes, not to necessary account data or the school's statutory records.

4.2 Excluded analyses

No advertising, no data trading, no training or fine-tuning of AI models with lesson content. No voiceprints, individual personality or performance profiles, speaking-time, emotion, behaviour or attendance analysis. Technical operating statistics must not allow an assessment of individual students or teachers and are not transmitted to the provider.

Processing in the classroom

5. Data flow and content filter

1. **Activation:** The teacher activates speech processing only for agreed lesson segments. The active state is recognisable; a stop ends the capture.
2. **Local recognition:** Speech is converted into text on the school server. At no time is a stored audio file created, not even for maintenance or troubleshooting.
3. **Filter before filing:** Names from the class, private details and off-topic statements are removed. This includes, for example, calling out names, toilet requests, private conflicts, health information and organisational interjections unrelated to learning.
4. **Subject-related learning note:** The cleaned subject-related content is stored. Historical or literary names needed for the subject matter, for example in a history topic, remain possible. The original personal statement is not kept alongside it.
5. **Search and answer:** Only approved content of the authorised course enters the search and the local AI. Personal chats, security logs and withdrawn content are not shared learning sources.
6. **Deletion:** Unprocessed text is discarded after filtering, at the latest five minutes after capture. Sources and the search data generated from them are deleted after the same period set by the school.

If the filter fails, this must not trigger unfiltered filing or publication. Segments that cannot be processed safely are discarded. Private content is also not copied into diagnostic logs, test data collections or backups.

6. Optional review and subject-related limits

Teachers can check, correct or delete notes. The review is optional; there is no mandatory approval step for every note. Learning notes may therefore be visible before a human review. Automatic filters can miss information, and AI content can be incorrect or incomplete.

The school sets up an accessible reporting channel. Reported personal or incorrect content is examined and, where necessary, blocked, corrected or deleted, including its derivatives. A notice about possible AI errors replaces neither effective technical filtering nor the handling of reports.

The AI supports learning and revision. It makes no decisions about grading, progression to the next year or admission and creates no automated personal performance assessments. Source-based lesson content and supplementary general explanations must remain distinguishable.

6.1 Protection of everyone present

Before use, students, teachers and other affected persons are informed. Private conversations are excluded from capture. Anyone who must not be captured needs a genuinely effective solution in the room; not creating an account or merely changing seats is not enough. If necessary, speech processing remains switched off.

Encryption

7. All files protected in storage and in transit

All files and data of the local school installation are encrypted at rest and in transit. This requirement covers all storage locations and network paths of the application, including backups, temporary files and administrative access.

7.1 Encrypted storage devices and data volumes

The physical storage media or data volumes are encrypted before school data is stored on them. This includes databases with their change logs, uploaded materials, learning notes, search indexes, account data, security logs and temporary files, insofar as they may be created at all. This does not make audio and raw text permitted stored holdings.

Suitable methods are, for example, **LUKS2 with dm-crypt on Linux** or **FileVault on macOS**. External drives, additional volumes, backups, snapshots as well as swap and hibernation files are considered separately. An encrypted system drive alone does not prove that all further storage locations are encrypted.

Backup copies are kept exclusively on encrypted, separately protected local media. There are no unencrypted copies on removable media and no automatic cloud synchronisation. The specific platform, the volumes covered and the method chosen are documented for the installation.

7.2 Encrypted transmission

Browser access takes place over **HTTPS/TLS**. All further network paths, including the microphone endpoint to the school server, internal services over the network, backup transfer and approved remote maintenance, must be authenticated and encrypted. Certificates and remote endpoints are verified; an error must not trigger a fallback to an unencrypted connection.

Approved remote access additionally uses the secure access controlled by the school. Mere membership of the school network or a Wi-Fi password does not replace the examination of the individual transmission paths. A device connected purely physically is assessed as its own local connection and protected against unauthorised access.

7.3 Keys, recovery and limits

The school determines the persons responsible for keys and recovery. Recovery keys are kept separately from the protected storage medium and accessible only to authorised persons; no filing in the general document area and no uncontrolled deposit in a private cloud account.

During setup, locked storage media, restart, unlocking, withdrawal of permissions and the recovery of an encrypted backup are tested. When media are replaced or decommissioned, data and keys must be deleted in a controlled manner.

Storage media encryption protects in particular a locked, lost or removed storage medium. Authorised running applications must be able to process content. Access protection, secure end devices, content filtering and deletion therefore remain additionally necessary. The public PDF itself requires no password.

Access and further protective measures

8. Roles and permissions

Role	Permitted scope
Students	Learning content of their own authorised courses; their own AI questions, where approved. No access to other people's chats, administrative functions or complete verbatim records of lessons.
Teachers	View learning content of their assigned courses and optionally check, correct or remove it. Access to individual task histories requires a separate school purpose explained in advance and the appropriate permission.
Parents and guardians	No automatic access. Separately permitted read access is limited to the assigned content and does not allow general observation of the class or of other people's conversations.
School management / administration	Named responsibilities for approvals, course permissions, blocking and justified individual checks. An administrative role does not justify analysing all learning interactions without cause.
School IT	Required technical maintenance, backup and recovery with limited privileged rights. No independent pedagogical analysis of content.
Provider support	Only specifically instructed, time-limited access. No permanent connection, no self-approval and no private use of lesson content.

8.1 Technical enforcement

Course and role permissions are checked on the server for every query, search, display and change. A visible button or valid access alone is not enough. Withdrawal of permissions also ends existing sessions and access to withdrawn content.

Login data is stored in protected form; passwords are not stored in plain text. Privileged accounts receive an additional authentication factor or equivalently secured procedures. Technical accounts receive only the rights necessary for their task. Secret access values do not appear in learning content or logs.

8.2 Operation, end devices and availability

Servers and backup media are located in an area protected against unauthorised entry. Network exposure is limited to necessary services; database, model and storage access is not opened directly to students or home networks. Security updates, responsibilities and recovery procedures are documented.

Reading and interactive AI questions are separate approvals. Home access does not allow anyone to listen in and does not switch on microphones. The application does not create permanent copies of content in browser databases or offline caches. Schools regulate secure end devices and signing out; screenshots or privately created copies cannot be completely prevented by technical means.

In the event of outages, a suitable learning alternative is available. There is no automatic switch to external AI services. New functions and changed data paths are assessed under data protection law before activation.

Retention periods and deletion

9. The school decides; the default is one school year

The school determines the retention period of learning content. The default is one school year: deletion at the end of the respective school year. In the regular Bavarian school year 2026/27 this is 31 July 2027. Content added later does not automatically receive another twelve months. The basis for the school year boundary is [Art. 5 BayEUG](#).

A shorter period can be set. Longer storage requires a purpose that remains permissible and necessary and is explained in advance. Mere later retrieval does not extend any period. The limits below are product requirements; stricter applicable requirements take precedence.

Holdings	Period / deletion event
Audio	No stored audio files, no archive and no backup copies.
Unprocessed text	Discarded after filtering, at the latest five minutes after capture. No backup.
Learning content and derivatives	Notes, materials, stored questions/answers and associated search data: deletion date set by the school, by default the end of the relevant school year.
Access and accounts	Blocked when the authorisation ends; deletion of the required account data at the latest 30 days afterwards.
Security logs	Access events at most 7 days; special administrative events such as changes of permissions at most 30 days. In each case without lesson or conversation content.
Backups	Encrypted, rolling, at most 14 days. No onward copy into an indefinite archive. Deleted data must not become accessible again through a restore.
Anonymous operating statistics	Only genuinely anonymous aggregate figures, insofar as the school permits them. Period determined by the school, by default the end of the school year; no individual history or transmission to the provider.

9.1 Complete deletion chain

On deletion, the content is first excluded from display, search and AI retrieval. Then the source, versions, derived notes, index entries, files and permitted caches are cleaned up. Deleting only one visible note is not enough if its derivatives remain retrievable.

An existing backup can still contain a copy that is no longer accessible for use for at most 14 days. Before a recovery is approved, deletions and withdrawals of permissions made in the meantime are applied again. Failed deletion runs are repeated and checked.

The school keeps any required legal records of consents, approvals or data protection cases separately, in line with the period applicable to each. They do not justify a blanket lesson or audio archive in ContextFriend.

Recipients, remote access and maintenance

10. No external processing of lesson content

For this local version, external AI services, cloud storage, content tracking and the use of lesson data by microphone or model manufacturers are excluded. The application uses the content exclusively for the purposes set by the school. Obtaining a model or a software update does not transmit any lesson content to the supplier.

Access is granted only to the persons authorised for the respective course and purpose and, where applicable, to expressly instructed technical bodies. The school names the service providers actually used and their roles in its school-specific notices. Further processors are engaged only on the required contractual basis and in accordance with the agreed approval procedure.

10.1 Access from home

Home access is approved exclusively by the school. The connection leads in encrypted form to an endpoint controlled by the school and opens only the permitted application, not general access to the school network. Reading alone does not yet permit interactive AI questions.

Permitted texts are displayed on the signed-in end device; this display then takes place outside the school building. Network operators can see connection metadata. The AI and the authoritative data remain on the school server. No transfer of lesson content to bodies in third countries is provided for in this version; deviating access must not be enabled tacitly.

10.2 Provider access only in individual cases

TamerinTECH has no permanent access to lesson data. Technical support is carried out without access to content wherever possible. If access to data is required in an individual case, the school first defines the purpose, the instructed person, permissions, duration and permitted tools. Where personal data is processed on behalf, the required contract for processing on behalf (Art. 28 GDPR) is in force beforehand.

Remote maintenance takes place in encrypted form to a secured, managed support device in Germany. Copies of content, downloads, printing, recordings and transfer into external ticket systems or AI tools are not permitted. The session ends when the task is completed, the agreed window expires or the instruction is withdrawn; remaining rights are revoked. If the available safeguards are insufficient, maintenance takes place on site.

A maintenance record documents the reason, the authorised person, the period and the measures carried out, without including lesson content. Support is not permission to record audio or to create a separate test and training collection. A private school role held by a provider employee does not give rise to additional provider rights.

10.3 Backup and changes

Backups remain on separate, encrypted media in the local protected area defined by the school. Responsibility, backup scope, recovery objectives and regular recovery tests must be documented. Risks of a failure of the entire site are assessed separately; they do not permit a covert cloud copy.

Changes to models, functions, permissions, storage locations, periods or recipients are assessed before they are used and updated transparently in the notices. An update must not tacitly extend the protection concept described here.

Rights and data protection incidents

11. Rights of data subjects

Under the statutory conditions, there are rights of access, rectification, erasure, restriction of processing and, where applicable, data portability. Where processing is carried out for a public task, an objection may be lodged on grounds relating to the particular situation. Consents given can be withdrawn for the future. The relevant rules are set out in Art. 12 to 22 GDPR.

The responsible school or its data protection officer receives requests. Identity is verified only to the extent necessary. The response is given as a rule within one month; any legally permissible extension and its reasons are communicated in good time. A refusal is justified and accompanied by the prescribed information on legal remedies.

TamerinTECH supports the school where it processes data on its behalf, but makes no independent decision about the release of third-party lesson data. Data subjects do not have to work through technical settings to raise their concern.

11.1 Complaint options

Responsibility	Contact
State schools in Bavaria	Bayerischer Landesbeauftragter für den Datenschutz (Bavarian data protection authority) PO Box 22 12 19, 80502 München Visitor address: Wagnmüllerstraße 18, 80538 München Telephone: +49 89 212672-0 poststelle@datenschutz-bayern.de www.datenschutz-bayern.de
Non-public bodies in Bavaria	Bayerisches Landesamt für Datenschutzaufsicht (Bavarian State Office for Data Protection Supervision) PO Box 1349, 91504 Ansbach Visitor address: Promenade 18, 91522 Ansbach Telephone: +49 981 180093-0 poststelle@lda.bayern.de www.la.bayern.de

For schools with a different maintaining body or special responsibilities, the school names the competent supervisory authority. The authorities offer secure online forms for complaints. The provider's contact point and the supervisory authority are different bodies.

12. Errors and security incidents

Unintended disclosure, unauthorised access, loss or other personal data breaches are reported without delay through the school's reporting channel. The responsible bodies limit access, secure the required evidence with minimal content and examine consequences and remedies. Affected learning content is blocked where necessary.

The controller examines a notification to the supervisory authority under Art. 33 GDPR, as a rule within 72 hours of becoming aware, where the notification obligation applies. Where there is likely to be a high risk, data subjects are informed under Art. 34 without undue delay. A processor informs the controller without delay after becoming aware.

Restart and recovery take place only after the protective measures, permissions and deletion requirements have been checked. A disruption justifies neither an audio recording nor the uncontrolled disclosure of school data.

Binding effect and sources

13. Setup at the school and maintenance of the documents

For every school, the actual delivery state, functions, devices, models, data paths, periods and responsible bodies must be established. The school prepares its specific notices and the required record of processing activities. It examines the obligation to carry out a data protection impact assessment; if a DPIA is required, it must be completed before processing. A remaining high risk must be handled under Art. 36 GDPR.

During setup, the following in particular are checked and documented at every installation: no audio storage even in the event of errors, filtering before storage, the five-minute limit for raw text, encryption of all storage and transmission paths, effective course permissions, correction and withdrawal, and deletion including backups. The absence of a mandatory review by teachers must be expressly taken into account in the risk assessment.

The school management decides on use together with the responsible school bodies. Data subjects are informed before the start; required consents are obtained separately. Subject-matter competence and age-appropriate support in the use of AI must be ensured. This concept contains no state approval or funding commitment.

Version 1.3 of 16 October 2026 applies together with the summary version of the same date. Changes are documented transparently. The public PDFs contain no completed school, contract or application documents. The school receives the contract and operating documents it needs separately.

14. Legal and technical sources

1. [General Data Protection Regulation](#), in particular Art. 5, 6, 9, 12 to 22, 25, 28, 30, 32 to 39.
2. [Art. 85 BayEUG](#) on the processing of personal data; [Art. 5 BayEUG](#) on the school year boundary.
3. [§ 46 BaySchO with Annex 1](#) on school processing activities; further provisions relevant to the respective school remain to be examined.
4. [Bavarian State Ministry of Education \(Kultusministerium\): Artificial Intelligence](#), with the guidance for pedagogical practice of 19 May 2026.
5. [§ 38 BDSG](#) on the designation of data protection officers by non-public bodies; this examination must be carried out independently of this contact information.
6. [Linux kernel documentation: dm-crypt](#) and [cryptsetup/LUKS](#); [Apple: FileVault](#). Descriptions of methods do not replace an examination of the installation.
7. Contact sources: [ContextFriend Impressum](#), [BayLfD](#) and [BayLDA](#). Retrieved: 14 October 2026.

Privacy contact at the provider

TamerinTECH GmbH · Seestr. 19 · 83727 Schliersee · Germany
hello@context-friend.com · +49 8026 387 25 98

For lesson data, please contact the responsible school or its data protection officer. The simplified family information and this full privacy concept are available at context-friend.com/school-documents.