Technical and organisational measures (TOMs)

Version of 12 November 2026 · Translation for information. The German version is binding.

Preliminary note

The measures are structured according to the protection goals of the Standard Data Protection Model of the German data protection supervisory authorities. SchuleVernetzt is developed and operated by SavePaperwork as a one-person business.

1. Data minimisation

- Pupils do not have an account. Only their first name, surname and class are kept; no date of birth, no address, no telephone number, no photo.
- A reason for illness is only asked for if the school switches this on; the question is switched off by default. For absence reports from teachers, a reason is never stored.
- Schools can switch off the upload of doctor's notes; for schools in North Rhine-Westphalia, Brandenburg and Berlin it is switched off by default.
- Notifications contain as little as possible: a message notification names only the sender, not the subject or text; a doctor's note reminder on the lock screen names no child.
- The school authority (Schulträger) account sees only school names and key figures, no persons.
- The class link and the foyer screen show no pupil names and no absent teachers.
- Deletion per type of data according to the periods of the federal state, once the school leadership has confirmed them.
- Read access entries in the audit log are deleted after 90 days (except records of answered access requests), application logs after 14 days; the school's audit log stores no IP addresses.
- The hosting provider keeps access logs with the full IP address for up to 90 days and error logs for up to 7 days, to investigate faults and fend off misuse.
- No analytics or tracking services and no third-party fonts run on the school's pages, nor in the school's emails.

2. Availability

- Operation in an ISO 27001-certified data centre in Frankfurt am Main (according to the hosting provider).
- Daily backup by the hosting provider, AES-256-encrypted, in a separate data centre in Helsinki, retained for 90 days.
- New versions are switched over atomically; a rollback to the previous version is possible at any time. Changes to the database schema are never applied automatically.
- Automatic monitoring every five minutes (database, background jobs, accumulations of errors) with alerts to the operator's phone.
- The class register can still be kept during a network outage; entries are submitted as soon as the device is back online.
- The school can itself download a complete export of all data at any time, even after the end of the contract (export guarantee).
- The target is an availability of 99.5% as an annual average, excluding announced maintenance.

3. Integrity

- Encrypted content uses authenticated encryption; any alteration is detected on reading and never silently accepted.
- The audit log records who created, changed or deleted a record and when, with the old and the new value; sensitive values are redacted in it.
- Forms are protected against cross-site request forgery; input is validated on the server.

- Uploaded files are checked for type and content (PDF, JPG, PNG, WebP, DOCX; at most 10 MB; no double extensions) and stored under a random name.
- Every change to the code goes through automated tests, including tests of the separation between schools.

4. Confidentiality

- Roles and permissions: the school leadership sees everything; the school office only what has been expressly released to it; teachers only their classes and subjects; parents only their own children. Only the school leadership, the school office and the class teacher can read the reason for illness, and every read access to it is logged.
- Separation of schools: all data belong to exactly one school; every query is limited to that school.
- Encryption in the application (libsodium; XSalsa20-Poly1305 for fields, XChaCha20-Poly1305 for files) for reasons for illness, grade values and comments, report card texts, class register entries about pupils, messages and all uploaded files. The key is held only in the server configuration; the file storage provider receives only ciphertext.
- Transmission exclusively via HTTPS with HSTS; session cookies only over HTTPS and not readable by scripts.
- In the school's areas a Content Security Policy allows only the platform's own scripts; injected code is not executed by the browser, and no other site can embed these areas.
- Passwords only as a hash (bcrypt or Argon2); sessions are ended when a password is changed; password reset links are valid for 24 hours and can be used only once.
- Protection against guessing attacks: at most five consecutive sign-in attempts, plus a computational puzzle (ALTCHA) without a third-party provider.
- Second factor (TOTP) mandatory for the school office and the school authority, available for the school leadership, plus passkeys. Teachers and parents can switch the second factor on as well; the school can require it for its teaching staff. Schools can set up the school sign-in (OIDC, for example Microsoft Entra, Google or a federal state login) and use its multi-factor authentication.
- Files are kept in private storage without public access and are delivered only through the application after a permission check.
- Application logs can be read only by the operator; a filter removes addresses, parameters, secrets and tokens before anything is written.
- The server's access credentials are kept only in a protected configuration file; development and test environments cannot reach the production storage.
- The operator accesses a school's data only where operation, troubleshooting or a request from the school requires it; the operator is bound to secrecy under § 203 StGB (German Criminal Code). If the operator signs in as a person of the school via the “Switch user” function for this, the operator's actions appear in the school's audit log as “Operator (SavePaperwork)” with the operator's name, not as actions of that person.

5. Unlinkability (purpose limitation)

- The data are processed only for the school: no advertising, no profiling, no disclosure, no training of AI models; no AI services are integrated into the school product.
- A school network shares nothing until each school joins and consents for each area (substitution pool, courses, materials); the requesting school sees a supply teacher's contact details only after they have been released. Leaving the network blocks access immediately.
- Production data of schools are never copied into development or test environments; there, the operator works with fictitious sample data.

6. Transparency

- In the audit log, the school leadership sees who changed which data and who opened which lists containing sensitive data.
- The agreement, the measures, the subprocessors, the retention periods per federal state, templates for the impact assessment and the record of processing activities, and information notices for parents, staff and pupils are publicly available.
- New subprocessors are announced 30 days in advance.

7. Intervenability

- Access and data portability: export of all data of a pupil or a parent with one click; export of the whole school at any time.
- The school itself carries out rectification, erasure and restriction in the application.
- The school itself determines retention periods, areas, the question about the reason for illness and visibility for parents; a class link can be renewed or switched off at any time.
- Notification of data breaches to the school without undue delay, as a rule within 24 hours.

8. Organisation

- SavePaperwork is a one-person business; the owner develops and operates the platform personally. Other persons are given access only after being bound to confidentiality and to § 203 StGB.
- New versions are deployed only by the owner, over the owner's own encrypted connection to the server.
- No data protection officer has currently been appointed; the contact person is the owner.
- These measures are reviewed with every material change to the platform and at least once a year.