Personal Data Protection Charter

Information for data subjects under Articles 12 to 14 of the GDPR

Version 1.0 **Date** 14 October 2026 **Publisher** Pass Technologie

1. Purpose

This charter describes how the personal data of Digital Workspace ("DWS") users is collected, used, retained and protected.

It is drawn up in accordance with Regulation (EU) 2016/679 of 27 April 2016 (GDPR) and French Act no. 78-17 of 6 January 1978 as amended, on information technology, data files and civil liberties.

2. Controller and processor

Data controller
The local authority and/or the head teacher, according to the split agreed in the DWS convention.

Processor within the meaning of Article 28 GDPR
PASS TECHNOLOGIE, a limited liability company with share capital of €15,000.00, 21 rue de Fécamp, 75012 Paris, France, Paris Trade and Companies Register no. 442 063 939, which designs, hosts and operates the Platform on behalf of the controller.

Data protection officer (DPO)
Mr Nader Boutros — PASS TECHNOLOGIE, 21 rue de Fécamp, 75012 Paris, France — nader.boutros@pass-technologie.fr

Each school remains responsible for the processing it carries out through the DWS in the course of its public education duties.

3. Purposes and legal bases

Purpose	Legal basis	Details
Account and directory management (creation, activation, authentication, assignment to classes and groups)	Public interest task (Art. 6(1)(e) GDPR)	Populated from academic directories and school information systems.

Provision of teaching and school-life services (homework diary, timetable, absences, marks, skills, home-school diary)	Public interest task	Processing linked to statutory obligations to monitor schooling.
Communication between members of the school community (messaging, instant messaging, forums, blogs, news)	Public interest task	Exchanged content is the responsibility of its authors.
Document storage and sharing (document area, drop box, shared resources)	Public interest task	Individual storage quotas apply.
Service security: connection logging, intrusion detection, antivirus scanning of attachments	Legal obligation and legitimate interest	Never used for systematic individual surveillance.
Audience measurement and service improvement	Public interest task	Usage statistics produced with a self-hosted solution configured in consent-exempt mode.
User support	Public interest task	Handling of support requests and incidents.
Optional features (profile photograph, mood, public profile information, mobile push notifications)	Consent (Art. 6(1)(a) GDPR)	Withdrawable at any time from account preferences.

4. Categories of data processed

- **Identification data**: surname, first name, login, national student identifier where applicable, date of birth, title.
- **Schooling and affiliation data**: school, classes, groups, profile (student, legal guardian, teacher, staff), roles and subjects, legal guardianship links.
- **Contact data**: email address, mobile telephone number, postal address where necessary.
- **Authentication data**: password hash, activation code, strong authentication factors where applicable.
- **School-life data**: absences, lateness, sanctions, marks and assessments, comments, reminders and homework.
- **User-generated content**: messages, uploaded documents, publications, collaborative contributions.
- **Optional profile data**: photograph, mood, interests, freely entered information.
- **Technical data**: connection logs, IP address, timestamps, session identifier, browser and device type.

No data falling within the special categories of Article 9 GDPR is collected by the Platform, unless stated otherwise in the school's record of processing activities.

5. Source of the data

Data originates from:

- academic directories and school information systems, through automated feeds;
- entries made by school administrators;
- information entered by users themselves in their profile;
- content they produce or upload while using the services.

6. Recipients

Data is accessible only to those who need to know:

- the user themselves and, for a minor student, their legal guardians;
- school staff, strictly within the limits of their duties and of the permissions granted to them;
- DWS administrators of the school and of the local authority;
- authorised staff of the publisher, solely for operation, maintenance and support purposes, within its processor mandate;
- judicial or administrative authorities, upon a lawful request.

Data is never sold, nor used for commercial or advertising purposes.

Digital resource services accessible from the resources hub receive, where applicable, a technical identifier and the user's profile, to the exclusion of any other identifying data, under the conditions laid down by the national resource access manager (GAR).

7. Hosting and transfers

Data is hosted in France, within the European Union, by OVHcloud:

- **application servers**: OVHcloud data centre in Gravelines (Nord);
- **backup servers**: OVHcloud data centre in Roubaix (Nord).

No data is transferred outside the European Union. Should such a transfer be implemented, it would be subject to prior information and to the appropriate safeguards provided for in Chapter V of the GDPR.

8. Retention periods

Category	Period
User account and directory data	Duration of schooling or assignment, then three months after leaving the roll
User-uploaded content (documents, publications)	Until deleted by the user, and at the latest when the account is deleted
Internal messaging messages	Current school year, plus two months

School-life data (absences, marks, sanctions)	Periods set by applicable regulations and by the school
Connection logs	One year, in accordance with applicable regulations
Audience measurement data	Twenty-five months maximum
Backups (three separate backups)	• user activity audit: one year; • personal data: duration of schooling; • course materials: duration of the user's subscription.

9. Import from Google Photos

The DWS Video application lets users who wish to do so import a video from their Google Photos account. This feature is optional and is only triggered by the user.

- **Google data accessed**: only the videos the user selects in the Google Photos window (`photospicker.mediaitems.readonly` permission). The DWS has no access to any other content of the Google account, nor to the user's contacts or email address.
- **Use**: the selected video is copied into the DWS, encoded and attached to the user's video entry, exactly like a file uploaded from their computer. It is then subject to the retention rules for user-uploaded content.
- **No retained access**: the authorisation issued by Google is only valid for the duration of the import. It is neither stored in the DWS nor reused, and no Google account is linked to the DWS account. Each new import requires a new authorisation.
- **No sharing**: data obtained from Google is not transferred to any third party, is not used for advertising, and is not used to train artificial intelligence models.

The use and transfer to any other app of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements.

Users can revoke this access at any time from the "Security" page of their Google account (third-party apps with account access).

10. Security

The following measures are implemented:

- systematic encryption of communications (HTTPS/TLS);
- storage of passwords as non-reversible hashes, with a complexity policy adapted to the user's profile;
- protection against repeated authentication attempts (temporary lockout);
- fine-grained permission management by profile and by school, with data separation between schools;
- antivirus scanning of uploaded attachments;
- access logging and continuous monitoring of the platform;

- regular backups and tested restoration procedures;
- ongoing security maintenance of software components.

11. Cookies and trackers

The Platform sets the following trackers:

Type	Purpose	Consent
Session cookie	Maintaining the authenticated session	Not required (strictly necessary)
Interface preferences	Language, theme, display	Not required (strictly necessary)
Audience measurement	Anonymised usage statistics	Not required, the solution being configured in line with the CNIL exemption guidance

No advertising or social network tracker is set.

12. Rights of data subjects

Every data subject has the following rights: access, rectification, erasure, restriction of processing, objection on legitimate grounds, and portability for data provided on the basis of consent or of a contract.

Where processing is based on consent, that consent may be withdrawn at any time, without affecting the lawfulness of processing carried out beforehand.

These rights are exercised with the data protection officer: Mr Nader Boutros, nader.boutros@pass-technologie.fr. A response is given within one month, extendable by two months for complex requests.

The Platform also provides an export feature allowing each user to retrieve the data and content of their account.

Any person who considers, after contacting the controller, that their rights are not respected may lodge a complaint with the CNIL — 3 place de Fontenoy, TSA 80715, 75334 Paris Cedex 07, France — or online at www.cnil.fr.

13. Data breaches

In the event of a personal data breach likely to result in a risk to the rights and freedoms of individuals, the controller notifies the CNIL within 72 hours and, where the risk is high, informs the data subjects as soon as possible.

14. Amendment of this charter

This charter may be updated to reflect changes in processing operations or in regulations. The version in force is the one published on the Platform. Any substantial amendment is notified to users.