



Viking International School Data Handling and Protection Policy

Policy Last Reviewed: November 2025

Viking International School (“VIS”, “the school”) is committed to protecting the personal data of students, parents, employees, volunteers, and all individuals associated with the school in compliance with:

- **EU General Data Protection Regulation (GDPR)**
- **Databeskyttelsesloven (Danish Data Protection Act)**
- **CPR-loven (Civil Registration Number Act)**
- **Barnets Lov**
- **Serviceoven**

This policy explains **what data VIS processes, how and why it is processed, how long it is kept, and what rights individuals have.**

The school maintains a **Record of Processing Activities (ROPA)** internally in accordance with GDPR Article 30.

2. Data Controller & DPO Contact Information

Data Controller:

Viking International School
Agernhaven 2K
2750 Ballerup
CVR: 40934073
Email: apply@vikinginternational.dk
Phone: +45 30555118

Data Protection Officer (DPO):

Angelika Cullen
Email: ancn@vikinginternational.dk

The DPO oversees compliance, advises VIS on data protection, conducts internal audits, and acts as the contact point for Datatilsynet.

3. Categories of Personal Data VIS Processes

VIS collects and processes the following categories of data.
(Full details are documented in the VIS ROPA.)

3.1 Ordinary Personal Data

- Student and parent names, contact details, addresses
- Date of birth, class, year group
- Attendance and behaviour records
- Internal communication logs
- Photos and videos (see photography section)
- Academic progress documentation
- Trip participation records

3.2 Sensitive Personal Data (GDPR Art. 9)

- Health data (allergies, medical needs, medication)
- CPR numbers
- SEN/PPR assessments and learning needs
- Psychological assessments
- Welfare concerns
- Safeguarding/child protection data
- Ethnicity or religion (only where relevant, e.g., dietary requirements)

Sensitive data is processed under **GDPR Article 9(2)** (b), (c), and (g) and relevant sections of **Serviceoven** and **Barnets Lov**.

3.3 CPR Numbers (CPR-loven)

Collected only when legally required for:

- Payroll
- SKAT reporting
- NemLogin-based services
- Udbetaling Danmark
- Municipality reporting
- Student enrollment

3.4 Employee Data

- Employment contracts
- Qualifications
- Background checks (including **børneattest**)
- Payroll and tax details
- Absence records
- Professional development
- IT access and logs

3.5 IT System & Device Data

- Login records
- IP logs

- Device identifiers
- Use of educational software
- Security logs (GDPR Article 32 requirement)

4. Photography & Video

VIS distinguishes between:

✓ Internal use (NO consent needed)

- Classroom documentation
- Internal communication
- Learning records (e.g., Toddle)

✓ External publication (CONSENT REQUIRED)

- Website
- Social media
- Marketing materials
- External publications

Consent may be withdrawn at any time without affecting prior lawful processing.

5. Legal Basis for Processing

VIS processes data under the following GDPR bases:

5.1 Contractual necessity (Art. 6(1)(b))

- Delivering education
- Managing enrolment and student records
- Providing communication to parents

5.2 Legal obligations (Art. 6(1)(c))

- Friskoleloven
- Serviceloven (safeguarding/underretninger)
- Arbejdsmiljøloven
- Tax & accounting laws
- Accident reporting
- Employment law
- Documentation required by Kommune or Ministry

5.3 Public interest / educational obligation (Art. 6(1)(e))

Schools serve a delegated educational role under Danish law.

5.4 Legitimate interests (Art. 6(1)(f))

- IT security
- Fraud prevention
- Managing operations

- Campus security
- (A balancing test is documented in the ROPA.)

5.5 Consent (Art. 6(1)(a))

Used only for:

- External photo/video publication
- Optional school activities or services

Consent can be withdrawn at any time.

5.6 Sensitive data — Art. 9(2)

Sensitive data is processed under:

- **Art. 9(2)(b)** – social protection & education
- **Art. 9(2)(c)** – vital interests
- **Art. 9(2)(g)** – substantial public interest
- **Art. 9(2)(a)** – explicit consent (limited cases)

6. How VIS Collects Data

- Directly from parents/students
- Teachers and school staff
- Through digital learning platforms
- From Kommune (PPR, safeguarding, social services)
- From job applicants and employees

7. Automated Decision-Making

VIS **does not** use automated decision-making or profiling under GDPR Article 22.

8. Data Sharing

Personal data is shared only when necessary and lawful.

8.1 Public Authorities

- Municipality (Børn og Familie, PPR)
- Police or emergency services
- SKAT & Udbetaling Danmark
- Ministry of Education
- Social services in safeguarding cases

8.2 Third-Party Processors

VIS uses the following main processors:

- Microsoft 365
- Toddle
- OpenApply
- Personio
- Komit / VIS Library System
- Approved educational tools

All processors have signed a **Data Processing Agreement (DPA)**.

8.3 International Transfers

If data is transferred outside the EU/EEA, VIS ensures:

- Adequacy decision, OR
- Standard Contractual Clauses (SCCs) with
- A Transfer Impact Assessment (TIA)

9. Retention & Deletion

VIS stores data only as long as necessary.

A detailed schedule is kept in the ROPA.

Summary:

Data Type	Retention
Safeguarding records	Until the child turns 30
Accident reports	10 years
Academic records	5 years
Admissions records	3 years after application
Behaviour & welfare documentation	5 years
Photos/videos	Until consent withdrawn or student leaves
Parent communication	3–5 years
Employee HR files	5 years after employment ends
Payroll/tax	5 years (Bogføringsloven)
IT logs	6–12 months

Deletion uses secure digital and physical destruction methods.

10. Security Measures (Technical & Organisational)

Technical

- Multi-factor authentication (MFA)
- Encryption at rest & in transit
- Access controls & role-based permissions
- Secure cloud environments
- Audit logging
- System monitoring
- Encrypted email for sensitive data
- Secure backup and disaster recovery

Organisational

- Annual GDPR training
- Acceptable Use Policy
- Confidentiality agreements
- Restricted physical access
- Processor review at least annually
- Clear onboarding/offboarding IT procedures

11. Staff Responsibilities

Staff must:

- Use only VIS-approved systems
- Never store VIS data on personal devices or personal cloud
- Encrypt sensitive data sent via email
- Protect login credentials
- Lock screens when unattended
- Report breaches immediately
- Ensure paper documents are stored securely
- Report lost devices immediately

12. Parent Responsibilities

Parents must:

- Provide accurate personal information
- Update the school when information changes
- Use approved communication channels
- Respect confidentiality of other families' data

13. Student Responsibilities

Students must:

- Protect login credentials
- Use school IT systems responsibly
- Not share other students' information
- Follow VIS digital safety rules

14. Rights of Individuals

Students, parents, and staff have the right to:

- Access their personal data
- Request correction
- Request deletion (*where legally permitted*)
- Restrict processing
- Object to processing
- Data portability (where applicable)

Deletion is not possible when VIS must keep data to:

- Meet legal obligations
- Safeguard a child
- Maintain essential educational records
- Retain tax/employment data

Requests should be sent to the DPO.

15. Right to Complain

Individuals may file complaints with:

Datatilsynet

Carl Jacobsens Vej 35

2500 Valby

Website: www.datatilsynet.dk

Email: dt@datatilsynet.dk

16. Data Breach Procedure

If a breach (suspected or confirmed) occurs:

1. Staff notify the DPO immediately
2. DPO assesses severity
3. Entry is made into the breach log
4. Datatilsynet is notified within **72 hours** if required
5. Affected individuals are notified if there is high risk
6. Remediation actions are implemented

Examples of breaches include:

- Email sent to the wrong parent
- Lost device containing school data
- Unauthorised access to systems
- Data shared with an incorrect recipient

17. Link to the VIS ROPA

The following details are documented in VIS's internal **Record of Processing Activities (ROPA)**:

- Detailed retention periods
- System-specific access controls
- Full processor list
- Lawful bases for each activity
- Security controls
- Data flows
- Transfer Impact Assessments (if any)

ROPA is not published but is available to Datatilsynet or external auditors on request.

18. Review & Governance

This policy is reviewed:

- **Annually**,
- After significant system changes, or
- Following new legal guidance from Datatilsynet.

19. Contact Information

For questions or data requests:

Data Protection Officer:

Angelika Cullen

Email: ancn@vikinginternational.dk