AARHUS
INTERNATIONAL
SCHOOL

GDPR
The General Data Protection Regulation
(Persondataloven)

Data Policy
The objective of AIS's data policy is to protect students, parents, employees and board members' personal information against unauthorized use, in accordance with the Personal Data Protection Regulation.
It is also a goal that this security measure goes hand in hand with common sense. Resources and measures taken should be within reasonable limits. Security and risk should be balanced.

Data policy is under ongoing development. If anyone has questions, comments or suggestions for the policy, please contact administration@ais-aarhus.dk

Data flow personal data

Parent / Student Information
Registered in the student administration system before and after admission.
Everything is done digitally. Consent is obtained.
Student information is processed in the following administrative systems:

- OpenApply
- ManageBac
- Tabulex/UVSkole
- Seasaw
- e-Boks
- STIL

Information will be deleted when it is no longer relevant, usually when the students are above MYP5 age.

Employees and applicants
Information regarding current employers and applicants is registered in staff archives. Consent is obtained.
Personal information is processed in the following administrative systems:

- Proløn/DSA-Løn
- ManageBac
- Educa Personale
- www.ais-aarhus.dk
- STIL
- e-Boks
- Office365/OneDrive

Physical documents - staff folders are almost all digitalized. Expected to be completed autumn 2022.
Unsolicited applications are kept max. 2 years. Systematic erasure is done annually in July
Applications for vacancies are kept max. 1 year. Systematic erasure is done half-yearly in July and January.

Board members
Registered in the board archives in Office365/OneDrive. Consent is obtained.
Board information is dealt with in the following administrative systems:

- www.ais-aarhus.dk
- Office365/OneDrive

Security

Physical archives
Remaining physical archives are stored in the school administration office at Dalgas Avenue and at Bushøj under lock. Only relevant persons have access to the archives.
Storing physical documents outside these locations should be avoided. It must only take place when there is a concrete need for this. For example, when reading large amounts of documents.

Devices (iPads and laptops) provided by the school have been set up with a personal password, which is being changed once a year.
Storing personal data on local drives or other external storage media can only take place when relevant and when written consent is obtained.
Parents are asked for consent to share class lists with phone numbers and email addresses with other parents and for staff to be stored on private devices.
All the school's devices are reviewed annually by the IT department in order to ensure security and functionality.

Downloading and storing personal data on private electronic media can only take place when relevant and when consent is obtained.

Office365 - employees
The school's Office365 accounts are set with a password that changes at least once a year.
The storage of personal data must be limited to a minimum extent and time. The individual employee is responsible for cleaning up and deleting documents at least once a year.

Sharing personal information internally within the organization on Sharepoint must be minimized in scope and time. The individual employee is responsible for cleaning up and deleting documents at least once a year.

Sharing personal information outside employee and management circles can only be done when written consent is obtained.

Non-active Office365 accounts are deleted by the school one month following resignation.

Mail system Outlook (part of Office365):
Use of or storage in Outlook’s standard folders of personal information must be minimized in time and extent.
Sent mail must be deleted or moved to personal folders after max. 6 months.
Inbound mail containing personal-sensitive information that may be repository is moved within 14 days to folder-tagged personal information. The individual employee is responsible for systematic erasure / cleanup in this folder at least once a year
Deleted mail should be deleted after one month.

In case of need to exchange "secure mail" information with authorities or others, this may be done by

contacting the administration office. (note e-Boks currently only available for registered recipients).

Office365 - students
Students are made aware of “AIS IT policy” and teachers help them to be familiar with the rules for responsible handling of data. It is also a parental responsibility to pay attention to this.
Accounts will be deleted by the school 1 month after the students leave.

Other programs and apps - students
AIS only support/use and download GDPR compliant apps and programs. School licenses have to be approved by the PYP/MYP Coordinators.

Social media
AIS have a Facebook account where pictures and other information from the school is uploaded. Portrait pictures will only be uploaded when consent is obtained from parents/staff. All pictures are checked for parental consent.
AIS is aware that Facebook is a controversial media when it comes to personal data protection.
We will observe the ongoing debates and if necessary close down our account.

Approved by the Board on 7 September 2022.The policy is revised on a regular basis, if necessary, by the Head of school. The policy currently in force is available at www.ais-aarhus.dk. The policy should be approved by the Board every 2 years.