Information security and privacy policy (ISP)

Author:
Raymond Wannée

Date and version:
15 February 2022

Classification

Public	This document may be shared and published without restrictions
Internal	This document may only be viewed by employees and relevant cooperation partners of the HSV
Confidential	This document may only be viewed by a limited number of authorised/competent employees of the HSV.
Secret	Only the following persons are entitled to see this document: N/A.

Table of contents

Key terms

General Data Protection Regulation (GDPR)	The GDPR is a European information security and privacy law. The GDPR provides for, among other things: ● Reinforcement and extension of privacy rights; ● more responsibilities for organisations; ● the same, robust powers for all European privacy supervisors, such as the power to impose fines of up to 20 million euros.
Personal Data Authority (APD)	The APD is an independent administrative body that supervises compliance with the statutory regulations for the protection of personal data.
Personal data	All information regarding an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by means of an identifier such as a name, an identification number (BSN or personnel number), location data (address), an online identifier (IP address) or one or more elements that are characteristic of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.
Special personal data	Special personal data are data that provide information about: religion or life philosophy, race, political preference, health or sexual life. The processing of these data is in principle prohibited unless it can be demonstrated that one of the exception bases is met.
Data leak	Unlawful access to, destruction, modification and release of personal data.
Data processing	An operation or set of operations relating to personal data or a set of personal data, whether or not performed by automated means, such as collecting, recording, organising, storing, updating structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise transmission, dissemination or otherwise making available, aligning or combining, blocking, erasing or destroying data. destruction of data.

1. Introduction

In order to be able to offer good and modern education, supervise pupils, provide learning resources and guarantee the continuity/quality of the education and the operational management, we obviously need (personal) data of pupils, parents and employees.

The education sector is increasingly dependent on information and (mostly computerised) information facilities. The amount of information is also increasing due to developments such as personalised learning with ICT. This dependence on ICT and data brings with it new vulnerabilities and risks. It is important to take adequate measures in the area of information security and privacy (hereinafter "ISP") in order to reduce the consequences of these risks to an acceptable level and to optimally guarantee the progress of education and business operations.

1.1 Information Security

Information security means taking and maintaining a coherent package of measures to guarantee the quality aspects of the information provision.
These aspects are

- Availability: the extent to which data and/or functionalities are available at the right time.
- Integrity: the extent to which data and/or functionalities are correct and complete.
- Confidentiality: the extent to which access to data and/or functionalities is limited to those authorised to do so.

Insufficient information security can lead to unacceptable risks in the execution of education and in the operations of the institution. Incidents and breaches in these processes can lead to financial damage and loss of image.

1.2 Privacy

Privacy is about personal data. Personal data must be protected in accordance with current legislation and regulations. Protection of privacy regulates, among other things, under which conditions personal data may be used. Personal data are all data/information that can reasonably be traced back (directly or indirectly) to a natural person/individual. Processing is understood to mean any action relating to personal data. The law lists the following examples of processing: collecting, recording, organising, storing, updating, amending, retrieving, consulting, using, providing by means of transmission, dissemination or any other form of making available, combining, linking, blocking, erasing and destroying data.

The law distinguishes special personal data from ordinary personal data. These are data for which extra strict requirements apply from a legal point of view because of the sensitive nature of the data. Examples of special personal data are data that say something about someone's health, race, religion, political preference, criminal past, sexual life and participation in trade unions.

1.3 Integration of information security and privacy

The above shows that information security is an important part of privacy, while conversely, dealing carefully with personal data is necessary for information security. Both concepts stand side by side and are dependent on each other. The subject of information security and privacy is abbreviated to ISP. This policy is the basis for the approach to information security and privacy within the HSV.

1.4 Privacy by Design

Privacy by Design means that, as an organisation, during the development of products and services (such as information systems) we first pay attention to privacy-enhancing measures. Secondly, we take data minimisation into account: we process as little personal data as possible, i.e. only the data that is necessary for the purpose of the processing. In this way, we can technically enforce a careful and responsible handling of personal data.

1.5 Privacy by Default

Privacy by default means that we must take technical and organisational measures to ensure that, as standard, we only process personal data that is necessary for the specific purpose we want to achieve.

1.6 Proportionality and Subsidiarity

All our data processing should be tested against the requirements of (1) proportionality and (2) subsidiarity.
This means that we must consider whether:

1. the purpose of the processing is proportionate to the intrusion for the individuals whose personal data we are processing

and

2. whether we cannot achieve the purpose in a way that is less intrusive for the individuals concerned.

1.7 Registration of processing activities: Data register

Under the General Data Protection Regulation (GDPR), every educational institution and more explicitly every data controller has an accountability obligation. This also means that educational institutions must be able to demonstrate that they act in accordance with the GDPR. Maintaining a register of processing activities (Data Register) is part of this accountability obligation. The register of processing activities contains information on the personal data that are processed within or on behalf of the educational institution. The HSV has a data register and is available for inspection by anyone upon request.

2. Purpose and scope

2.1 Purpose

The main objectives of this policy are

1. Ensuring the continuity and quality of education and business operations;
2. Safeguarding the privacy of pupils, staff and all other parties involved with the HSV.

This policy is aimed at optimising the quality of the processing of information and the security of personal data, with a good balance between privacy, functionality and security. The starting point is that the privacy of the data subject, in particular of employees and pupils, is respected and that the HSV complies with relevant laws and regulations.

2.2 Scope

- The information security and privacy policy within the HSV applies to all employees, pupils, parents/guardians, (registered) visitors and external relations (hired / outsourced), as well as to all organisational units. This policy also covers all devices from which authorised access to the school network can be obtained.
- The emphasis of the policy is on those applications that fall under the responsibility of the HSV. The policy covers both controlled information generated and managed by the school itself. It also applies to non-controlled information to which the school can be held accountable, such as statements made by staff and pupils in discussions, on (personal pages of) websites.
- The policy relates to the processing of personal data of all those involved within the HSV, including in any case all employees, pupils, parents/guardians, (registered) visitors and external relations (hiring/outsourcing), as well as other data subjects whose personal data the HSV processes.
- The policy focuses on the, fully or partly, automated/systematic processing of personal data that takes place under the responsibility of the HSV as well as on the underlying documents that are included in a file. The policy shall also apply to non-automated processing of personal data which are contained or intended to be contained in a file.
- The ISP policy within the HSV has interfaces with:

- the security policy;
- Staff and organisation policy;
- IT policy;
- participation of pupils, their parents/carers and employees;
- policy on the purchase/purchasing and use of digital learning resources.

3. Starting points

3.1 General policy principles

The most important policy principles at the HSV are:

a. Information security and privacy must comply with all relevant laws and regulations, in particular all relevant Education laws and regulations and the General Data Protection Regulation. The processing of personal data is based on one of the legal bases. Whereby a good balance between the interest of the HSV to process personal data and the interest of the data subject to make his/her own choices with regard to his/her personal data in a free environment is important.
b. Within the HSV, the safe and reliable handling of information is everyone's responsibility. This not only includes actively contributing to the security of computerised systems and the information stored therein, but also of physical documents.
c. The competent authority (the director) is the owner of the information that is produced/stored/processed under his/her responsibility at the schools and therefore responsible for processing according to the GDPR. In addition, the school manages information whose ownership (copyright) belongs to third parties. Employees, parents and pupils must be properly informed about the regulations concerning the use of information.
d. Information has a value: financial, economic but certainly also emotional. The value of information is classified at the HSV. The classification is the starting point for the measures to be taken. Subsequently, possible risks are identified by means of a risk analysis, using the classification. There is a balance between the risks of what we want to protect and the required investments and measures. Appendix 2 provides a more detailed elaboration of this
e. The HSV concludes agreements with all external parties and partners if they receive personal data from or on behalf of the organisation. If possible, use is made of the most recent version of the 'Digital learning resources privacy' processing agreement of the PO-raad. This also applies to government and other institutions if data of pupils or staff members is provided, whether or not on a legal basis.
f. It is expected of all employees, pupils, (registered) visitors and external relations that they behave in a 'decent' manner with their own responsibility. It is not acceptable that through intentional or unintentional behaviour unsafe situations occur which lead to damage and/or loss of image.
g. Information security and privacy at the HSV is a continuous process, which is regularly evaluated (at least annually) and it is determined whether adjustments are required.
h. When changes are made to the infrastructure or when new (information) systems are purchased, the HSV takes information security and privacy into account from the start. In these cases, a Data Privacy Impact Assessment (DPIA) is performed.
i. Safeguarding information security and privacy is an integral part of the quality assurance within the HSV.

3.2 Principles of information security and privacy

The six principles governing the handling of personal data at the HSV:

1. **Purpose and purpose limitation**: why do we process personal data and what do we do with the data? We process and share personal data for the following purposes in particular:

Teaching and organising;
Supervising pupils;
Providing learning resources;
Continuity of business operations;
Safeguarding security.

The information we collect is used exclusively for the stated purposes.

2. Basis: are we allowed to process data? We only process data on the basis of:
Legitimate interest
Public interest: performance of public tasks
Legal obligation
Execution of an agreement
Explicit consent
Vital interest

3. Data minimisation: do we have too much data? for example:
Only collect data that is really necessary to achieve the intended goals.
Only give people access to the minimum they need on the basis of their function
Not keeping data longer than strictly necessary

4. Transparency/ data subjects' rights: did we adequately inform data subjects? We strive to inform all our pupils, parents, employees and all other parties involved in an understandable way about the information we gather and their rights. For example by providing information leaflets at all schools, privacy statements on the website and by announcing fixed contact persons.

5. Data integrity: does collected personal data contain any errors? We ensure as much as possible that the data collected by us is kept up-to-date and does not contain any errors.

6. Information security: Technical and organisational measures: Have I taken the right measures to prevent the loss of personal data? For example: store pupil files in a lockable cupboard and lock the room when nobody is in it.

3.3 Quality control

Personal data must be adequately and proportionately secured according to generally accepted security standards. The quality requirements in accordance with ISO/IEC 27001(2) are pursued. ISO/IEC 27001(2) is a worldwide recognised quality standard for information security. The GDPR explicitly indicates that ISO/IEC 27001(2) can be an important tool for demonstrating the requirements and regulations from the GDPR. We do this by means of an annual evaluation based on this guideline.

The ISO/IEC 27001(2) is roughly structured as follows:

Category	Goal
1. Information security policy	The competent authority actively promotes the importance of information security, in accordance with relevant laws and regulations, and plays an active role in this, in word and deed.
2. Organisation of information security	Establishing a framework to initiate and control the implementation and execution of information security within the organisation.
3. Staff awareness	Ensuring that employees understand their responsibilities, during and after employment.
4. Asset/process management	Identifying and classifying information systems in the organisation and ensuring an appropriate level of security.
5. Access security	Preventing unauthorised access to systems and applications.
6. Cryptography (encryption)	Ensuring correct and effective use of cryptography to protect the confidentiality, authenticity and integrity of information.
7. Physical security	Preventing unauthorised physical access to, damage to, and interference with information and information processing facilities.
8. Security of operations	Ensuring correct and secure operation of information processing facilities and integrity of operational systems.
9. Communication security	Protecting information in networks.
10. Acquisition, development and maintenance	Adequate design and maintenance of information systems.
11. External and supplier relations	Safeguarding organisation information that is accessible to third parties.
12. Management of information security incidents	Effective incident management.
13. Information security aspects of business continuity management	Embedding information security in the organisation's quality management.
14. Compliance	Preventing violations of legal or statutory obligations.

4. Laws and regulations

At the HSV, we always strive to comply with all applicable relevant laws and regulations to the best of our ability, including:

- Constitution
- General Data Protection Regulation (GDPR)
- Primary Education Act and Expertise Centres Act
- Good Education and Good Governance Act PO/VO
- Archives Act
- Compulsory Education Act
- Copyright Act
- Penal Code
- Convention on the Rights of the Child (Article 26)

In addition, the provisions in the covenant 'Digital educational resources and privacy 3.0' of the PO Council are leading when making agreements with suppliers of educational software and student administration systems.

4.1 Board Policy

Below is an overview of other applicable board policy documents that are related to privacy and information security:

- Information security and privacy policy (ISP);
- Privacy protocol;
- Domestic violence and child abuse code;
- Complaints procedure;
- Whistleblowers' regulation;
- Non-discrimination statement;
- School and safety protocol;
- Code of conduct (for staff and pupils HSV);
- Personal and intimate care protocol;
- Absenteeism protocol;
- Visual material policy on the internet and school apps;
- Social media protocol;
- Data breach protocol;
- COVID-19 protocol;
- Smoking policy.

5. Organisation

The organisation of ISP is about processes, habits, policy, laws and rules that are of significance for the way in which people steer, manage and control an organisation. The relationships between the different people involved and the objectives of the organisation play a role in this.

This chapter describes how ISP is organised in the HSV. A distinction is made between three levels:

- Guiding (strategic)
- Directing (tactical)
- Executive (operational)

For each level, there is a description of which roles have which responsibilities and tasks, and what the documents are that match.

5.1 Roles and responsibilities

To tackle information security and privacy in a structured and coordinated way, the HSV recognises a number of roles that have been assigned to employees in the existing organisation.

a. Directing

Ultimately responsible
The Board is ultimately responsible for ISP and determines the policy and the basic measures in the field of information security and privacy. The application and functioning of the ISP policy is evaluated on the basis of regular reports. The substantive responsibility for ISP is mandated to the DPO and policy responsible person(s).

b. Steering

Data Protection Officer
The Data Protection Officer (DPO) supervises the application of and compliance with the GDPR within the HSV. The legal tasks and competences, in accordance with the guidelines of the Personal Data Authority, of the DPO give this officer an independent position in the organisation. The DPO has regular consultations with policy makers and those with final responsibility. The DPO is usually also the contact person for complaints and questions from data subjects. The DPO is a role at management level.

According to article 39 of the GDPR, the DPO performs at least the following tasks:

1. Informing and advising the organisation about their obligations in relation to the legal requirement for the protection of personal data.

2. Supervise compliance with the:
a. GDPR;
b. Other Union law (i.e. European) or national data protection provisions;

c. of the Board's policy regarding the protection of personal data (including
of responsibilities, awareness and training of employees, and the relevant
audits.

3. Giving solicited and unsolicited advice in relation to data protection

4. Cooperating with and acting as a contact point for the Personal Data Protection Authority (PDPA) on matters related to the processing of personal data, and - where appropriate - consulting on any other matter relating to privacy.

5. In the execution of his tasks, the DPO is obliged to take into account the risks associated with the use of personal
personal data, and of the nature, scope, context and objectives of the use of that data.
use of that data.

6. Raise and maintain awareness in the organisation.

The DPO collects information to:
Identify processing activities;
Analyse and monitor compliance of processing activities;
Inform, advise and make recommendations to the organisation;
Monitor uniformity within the HSV.

The DPO is:
The contact point for incidents/complaints in the field of information security and privacy.
Responsible for the further handling of incidents/complaints within the HSV.

The GDPR obliges the board to give the DPO access to all personal data and processing thereof. The DPO must also have the necessary resources at his disposal to carry out his tasks, and to maintain his expertise. The DPO must be actively supported in his work by the Board. The following starting points are maintained:

- Sufficient support in terms of financial resources, infrastructure (premises, facilities, equipment);

- Required access to other services, such as access to the files of human resources, the legal department, the ICT department etc. The DPO receives essential support, input and information from these employees or departments;

- The DPO must have the opportunity to keep up to date in the area of data protection, whereby the starting point must be that the level of knowledge rises continuously;

- The DPO is authorised - on his own initiative - to carry out research, to give (unsolicited) advice on this, and to demand cooperation from everyone in the organisation.

Policy officer(s)

The policy responsible persons advise the Board in cooperation with the DPO and are co-responsible for the organisation of information security and guarantee of privacy within the HSV. The policy officer(s) is/are also responsible for the adjustments in the policy documents.

School directors

School directors are responsible for translating the board policy into educational practice. For example, it may be necessary to produce additional guidelines, procedures, measures and documents at school level when the ISP does not provide for certain school-specific matters. Also the enforcement of the policy at school level is part of this responsibility.

More specifically
- mapping data processing/applications and software used.
- Identifying new data processing (e.g. new software) and taking adequate measures (checking in the data register or else reporting to the Data Protection Officer at the Executive Director).
- Applying for authorisations (rights to applications).
- Signalling and reporting data breaches within the school.

Domain manager / process owner

Within the board office there are several domains/processes such as: policy, ICT, HRM (salary and personnel administration, absenteeism and reintegration), secretariat, communication, procurement and facility management. Within these domains, the employees are responsible for determining how ISP is given shape within the working method used. In case of doubt, advice should be sought from the Data Protection Officer or policy officers.

Employees are also responsible within their domain for the risks that are caused by persons or applications that are wrongly accessed. To reduce these risks, process owners have the following specific tasks:

- Together with DPO and ICT, they ensure that users only get access to the network and the network services for which they are specifically authorised.
- Together with DPO and ICT, they regularly assess users' access rights.

c. Executive

ICT
The ICT forms a technical point of contact regarding information security for the organisation.
The ICT:

- Develops and manages the information systems;
- Manages the network;

- Supports and advises employees;

Functional managers

The functional administrators of applications (such as YouForce) are provided by the domain responsible / process owner with a completed work package, consisting of guidelines, procedures and instructions. On this basis he performs his or her tasks.

Employees

All employees have a responsibility in relation to information security in their daily work. These responsibilities are described in the deed of appointment, collective labour agreement, code of conduct and other management policies, among other things. Employees are asked to be actively involved in information security. This can be done by reporting (near) incidents/data breaches, submitting improvement proposals and exerting influence on the policy (individually or via the participation council). All employees also have the responsibility to report new data processing and to check this with the DPO.

Department heads

Compliance with the information security policy is part of the integral management. At the executive level, every manager has the task of

- ensuring that his/her employees are aware of the policy;
- supervising compliance with the ISP policy by the employees, whereby he/she himself/herself has an exemplary function;
- periodically bringing the subject of ISP to the attention of employees in work meetings, appraisals, etc;
- to be available as a contact point for all personnel-related ISP topics.

The manager can be supported in his/her task by the DPO and policy officers.

6. Monitoring and reporting

This information security and privacy policy is tested and adjusted at least every two years. The following is taken into account

- The status of the information security as a whole (policy, organisation, risks)
- The effectiveness of the measures taken and their demonstrable functioning

The HSV also has an annual evaluation cycle for information security and privacy. This is a periodic evaluation process that tests the content and effectiveness of the information security and privacy policy.

All consultation moments are fitted in as much as possible in existing consultation forms with the same character, whereby on the strategic level, directional discussions are held about the organisation and the policy:

- strategic level, directional discussions are held about the organisation and compliance, as well as about goals, scope and ambition in the field of ISP.
- tactical level, the strategy is translated into plans, standards, evaluation methods, etc. These plans and instruments are used to guide implementation.
- operational level: the subjects that affect daily operations are discussed. This form of consultation is organised decentrally, and if necessary in each organisational unit of the HSV.

6.1 Information and awareness

Policy and measures are not sufficient to exclude risks in the field of information security and privacy. In practice, people are usually the most important players. Therefore, at the HSV, the awareness of the individual employees is continuously sharpened, so that the knowledge of risks is increased and safe and responsible behaviour is encouraged. Regular employee awareness campaigns are part of the policy. Increasing security awareness is a responsibility of the DPO, policy makers and management/school directors with the director having final responsibility. During various management meetings, team meetings, professionalization meetings and school visits, attention was and is paid to information security and privacy.

6.2 Classification and risk analysis

At the HSV, all information has value, therefore all data to which this policy applies is classified (public, internal, confidential and secret). The level of security measures depends on the classification. The classification of information depends on the data in the information system and is determined on the basis of risk analyses. Availability, integrity and confidentiality are the quality aspects that are important for the information provision. See appendix 2.

6.3 Incidents and data leaks

All incidents can be reported to the DPO. The handling of these incidents follows a structured process, which also provides for the correct steps concerning the obligation to report data leaks. A separate protocol concerning data leaks is available on the intranet.

6.4 Monitoring, compliance and sanctions

Compliance consists of general supervision of the daily practice of the ISP process. It is important here that managers and process owners take their responsibility and address their employees in the event of shortcomings. At the HSV, attention is actively paid to ISP at the time of appointment, during the interview cycle, with an institution-wide code of conduct, with periodic awareness campaigns, and so on.

To promote compliance with the GDPR, the Data Protection Officer (DPO) plays an important role. The DPO is appointed by the board, and has a legally defined and independent supervisory role. The DPO will therefore carry out an annual investigation into possible irregularities in relation to the IPP and report on this to the Board.

If there is a serious lack of compliance, the HSV can impose a sanction on the responsible employees involved, within the framework of the CAO and the legal possibilities.

At the HSV, the reporting of security incidents and data breaches is laid down in a protocol/step-by-step plan. This can be found on the intranet.

6.5 Independent legal advice

The HSV is assisted by the dispute committee in case of conflicts. In case of more complex cases, the HSV will be assisted by a specialised law firm.

6.6 Featured topics

The following section highlights a number of themes that are often discussed in daily practice. For that reason, additional explanation of these themes is given below.

a. Password policy and settings

It is recommended to draw up a general policy for all systems with regard to password requirements.
It is recommended to draw up a general policy for all systems with regard to password requirements in accordance with the following guidelines:

- Minimum number of characters: 8
- Maximum validity period: 30-90 days
- Complexity: enabled
- Password history of 20 passwords
- Account lockout: 3
- Account lockout duration: more than 0 minutes

Hereafter, it is important to implement this policy on all relevant IT systems, and perform annual checks to verify that password requirements are still enforced in accordance with the password policy. In addition, adequate password management is important. Passwords should be stored in such a way that only the authorised/competent person has access to them. Where it seems proportionate, the ICT of the HSV can implement two-factor authentication (extra security).

b. Social media

Social media such as Twitter, Instagram, Facebook, YouTube and LinkedIn offer unique opportunities in relation to positive profiling of our schools.

The HSV trusts that employees, guest lecturers, pupils, parents/guardians and other parties involved use social media responsibly.

The HSV has drawn up a separate social media policy for our employees to ensure the best possible use. In addition, we make agreements with each other about what is not allowed. The most important principle in our activities in the field of social media is that we stick to the regular decency norms, just like in the 'real' world. The social media policy is published on the intranet.

c. Application use

If applications collect personal data, it is important to be critical of the privacy-friendliness of the application. Relevant questions are:
Is the application strictly necessary for providing education, guiding pupils, providing learning resources and continuity of the educational process?
Is there a legal basis for using the application?
Does the application collect too much data?
Is there a processing agreement with the supplier of the application?

Before working with an application, this application should be checked in the data register mentioned in Chapter 1.7. If the application is not listed, this application should be reported to the Data Protection Officer of the HSV.

d. Use of portable devices

It is recommended to be as cautious as possible in the use of portable devices for processing personal data. It is recommended that extra care be taken with the storage and security of portable devices. When working with a portable device, such as a laptop, it is important to work as much as possible in the secure Google environment. Portable devices should always be encrypted with a personal access code.

e. Use of e-mail

E-mail is an important means of communication in our organisation. However, a large proportion of data leaks are caused by the use of e-mail. It is therefore important to think carefully when choosing to use e-mail to transfer personal data. An alternative is to share files with colleagues via the Google environment. Employees should carefully check the e-mail addresses of the recipients of the e-mail. When sending mail to multiple parties, it is recommended to use the BCC.

f. Health care records

Care files are a source of special personal data and therefore contain very sensitive information. It is very important to handle these records with extra care. Only those professionals who, based on their contribution to the formulated care needs, need access to the files should be allowed to do so. It is the responsibility of the school director to determine who is entitled to access the data.

g. Leaving

Employees may no longer have access to the HSV's data processing when they leave the school. When leaving, a signal from the school concerned should be given to the IT of the HSV. The ICT ensures that the issued rights with regard to the access to data processing are withdrawn by the functional administrators. This applies to data processing/information systems/applications for which rights are issued centrally. Other data processing/information systems/applications are to be regulated by the School Board.

Data type	Legal basis	Explanation
1. Specific cases	Specific law	If the processing falls outside the situations described below, it is important to find the specific retention or destruction period in the applicable legislation and regulations. European subsidy incentive scheme
2. European subsidy incentive scheme		Information must be retained for 10 years after the departure of the pupils concerned.
3. Financial, tax and accounting documents	Art. 172 par. 3 PO Law Art. 130a par. 3 VO Law	7 years

4. All data in the pupil administration PO / VO	Article 9 paragraph 1 (in conjunction with Article 6 paragraph 1) Funding Decision WPO Article 6 Financing Decree, VO	Up to 5 years after the deregistration of the respective pupil.
5. Student file	Advice Authority Personal Data.	2 years after departure of pupil
6. Personal data concerning the health of pupils	Article 18a para. 6 (in conjunction with para. 13) P.E. Act 17a para. 14 Act VO	3 years after the end of: (a.) the assessment of whether a pupil is suitable for learning support education or of the admission of pupils to practical education or secondary special education (b.) the advice on the support needs of the pupil to the school's competent authority, (c.) the allocation of support resources or facilities to the school.
7. Application data	Advice Authority Personal Data	The advice of the Authority Personal Data (APD) is to delete the application data no later than 4 weeks after the end of the application procedure. It is possible to retain data for longer with permission. For example, because a suitable position may become available at a later date. A maximum period of 1 year after the end of the application procedure is reasonable according to the APD.
8. Administrative absence data/re-integration file	Advice Authority Personal Data	The APD states that a retention period of two years after the end of the employment/reintegration process is reasonable. But when there is, for example, a labour conflict, the employer can keep this data longer.
9. Other data traceable to persons		Erase 2 years after deregistration or termination of relationship.
10. If there is consent to keep data for a specific purpose after unsubscribing		Retention allowed on the basis of consent.

11. Not personally identifiable		Free to choose

Appendix 1. Plan of approach for information security and privacy

Action	**Planning**	**Completed**
The executive director knows in principle what information security and privacy protection are about		x
The executive director endorses the importance of Information Security and Privacy Policy (ISP)		x
The executive director knows what the GDPR means for an executive director.		X
The ISP has been: a. prepared; b. approved by the executive director c. and communicated to those concerned.		x
The ISP organisation is set up in such a way that responsibilities and tasks are assigned to employees.	x	
Privacy statement is confirmed		X
Basic ISP measures and access policy for data and applications have been approved and recorded	x	
Data Protection Officer (DPO) appointed		x
Evaluate application and functioning of ISP policy on the basis of reports.	x	
The executive director knows the background of the measures to be implemented		x

Data and processes are classified	Ongoing process	
The current situation has been surveyed. A risk analysis has been carried out.		x
A procedure for reporting security incidents (data breaches) has been ● Drafted ● Approved ● Communicated		X
A data breach and security incidents hotline has been published		X
Incident registration is in place		X
Rights of those involved are recorded and communicated to staff, pupils and parents		x
There is a process description how data subjects can exercise their rights		x
Privacy statement have been drawn up, adopted by the board and communicated		X
There is a confidentiality agreement for non permanent employees		X
There is a password policy		X
Agreements have been made with suppliers who process personal data (management and review of contracts) Processor agreements	Ongoing process	X
The Privacy insert of the processor agreements have been published (transparency)		X
Permission for parents/pupils to use visual material has been arranged		X
Procedure for withdrawing consent is established and communicated		X

Agreements and procedures on privacy are arranged and communicated (duty of information, transparency)		X
The processes surrounding Duty of Information is in place	X	
A social media protocol or code of conduct has been established. (with extra attention for pupils <16 years old)		X
There is an ICT and internet use code of conduct / Acceptable use policy		X
Agreements on appropriate education are made and known to the employees involved	X	
Agreements on youth assistance are made and known to the employees involved	X	
There are agreements on the exchange of pupil records and data with other schools	X	
Are the relevant staff aware of the rules on handling student files?	X	
Agreements on compulsory education and absenteeism are in place and known to the employees involved		X
Is there an Authorisation Matrix	Needs an update	X
The authorisations and roles of employees are defined (e.g. by means of an authorisation matrix)	needs an update	X
Employee authorisations and roles are entered and regulated in the administration systems	X	
There is a process to check authorisations	X	
The application and functioning of the ISP policy is evaluated on the basis of reports.	X	
A Data Protection Officer (DPO) has been appointed		X
There is monitoring of compliance with privacy legislation		X
New developments/technologies are examined in advance to determine whether they require a data protection impact assessment		X
A standard template of data protection impact assessment is available		X
Privacy by design, privacy by default are taken into account		X

All personal data registrations are demonstrable (documentation obligation, data register)	X	
There is an overview of all suppliers/externals that process personal data on behalf of the organisation.	X	
There is an overview of all applications in which personal data are processed (internal)		
Agreements concerning camera surveillance are arranged and communicated	X	
Measures have been taken to limit and/or prevent DDoS attacks	X	
There is a Cleardesk policy		X
Attention is paid to teacher ICT competence	X	
Pupils are informed about ISP at school	X	
Attention is paid to media literacy and digital literacy of pupils		X
Social media rules have been made known to all involved		X
Code of Conduct has been made known to all stakeholders		X
Parents are actively approached and informed about ISP at school and made aware of their rights		X
The (G)MR has been (is) regularly informed about ISP.		X
Security awareness training is given to all employees	X	

Appendix 2. BIV Classification

The quality aspects applied to information security are Availability, Integrity and Confidentiality. These terms are described here including the sub aspects. All aspects can be classified as low, medium and high.

Availability:

The extent to which control measures guarantee the availability and undisturbed progress of the ICT service.

Sub-aspects of this are:

- Continuity: the extent to which the availability of the ICT service is guaranteed;
- Portability: the extent to which the transferability of the information system to other similar technical infrastructures is guaranteed;
- Recoverability: the extent to which the information provision can be restored in time and in full.

Level 1: **Low:** availability is not important	**Level 2:** **Medium:** availability is important	**Level 3:** **High**: availability is necessary
The total loss or unavailability of this information for several days does not cause any noticeable (or measurable) damage to the interests of the institution, its staff or its pupils	The total loss or unavailability of this information during one day will cause noticeable damage to the interests of the institution, its staff or its pupils	The total loss or unavailability of this information during one workday will cause noticeable damage to the interests of the institution, its staff or its pupils

Integrity:
The extent to which the management measures (organisation, processes and technology) ensure the correctness, completeness and timeliness of IT services.

Sub-aspects of this are:

- Correctness: the extent to which the presentation of data/information in IT systems is consistent with reality;
- Completeness: the degree to which the completeness of data/information in the object is guaranteed;
- Assurance: the extent to which the correct functioning of the IT processes is assured.

Level 1: **Low:** integrity is not important	**Level 2:** **Medium:** integrity is important	**Level 3:** **High**: integrity is necessary
Continued accuracy of information (from source to final use) is desired, but not guaranteed. If information is not correct, this results in limited damage.	Continued accuracy of information must be ensured. Some tolerances are permissible. accuracy of information is important, but not critical. it is not necessary that accuracy can be demonstrated beyond doubt. if information is not correct, the organisation may suffer substantial damage.	Information where it is necessary that the correctness cannot be disputed, such as test results, exams, irreversible financial transactions. If information is not correct, the organisation may suffer serious damage.

Confidentiality:
The extent to which only authorised persons, software or equipment can use the data or software, whether or not regulated by (automated) procedures and/or technical measures.

Sub-aspects of this are:

- Authorisation: the extent to which the adequate organisation of authorisations is guaranteed;
- Authenticity: the extent to which adequate verification of identified persons or equipment is guaranteed;

- Identification: the extent to which mechanisms for recognising persons or equipment are ensured;
- Periodic checks on existing authorisations. The (automated) determination of whether identified persons or equipment are permitted to perform the desired actions.

Level 1: **Low:** information is for internal use	**Level 2:** **Medium**: information is confidential	**Level 3:** **High**: information is classified
Disclosure of data results in little or no harm to a concerned institution or data subject	the organization, institution or data subject can suffer substantial damage if information is accessible to unauthorized persons. information may only be accessible to persons who, due to their position, should have access to it (need-to-know basis). This includes personal data.	The organization, institution or data subject can suffer severe damage if information is accessible to unauthorized persons. Information must only be accessible to a very select group of people. This includes personal data.