Information security and privacy policy

Haagsche Schoolvereeniging

1 Introduction

Information and ICT are necessary in support of education. Because we work with personal data (of ourselves, students and others), privacy legislation applies to this.

The information and ICT of the HSV are exposed to a large number of threats, whether intentional or not. All information we store and process can be threatened by an attack, a mistake, nature (eg flooding or fire), etcetera. The unavailability of ICT, incorrect administrations and the leakage of data can lead to violations of education and confidence in our school.

These threats make it necessary to take measures to reduce the risks associated with these threats to an acceptable level. It is necessary that we make clear what it is about, set a goal and describe the way in which we want to achieve this goal.

1.1.1 Information security and privacy

Information security is a process for protecting the HSV against risks and threats related to information and ICT. It focuses on three aspects:

- Availabilty; information and related assets are accessible when necessary;
- Integrity; information and processing methods contain as few errors as possible;
- Confidentiality; information is only accessible to those who are authorized.

Privacy concerns the protection of personal data in accordance with current laws and regulations. By properly applying information security, this legislation can be met. Especially the aspect of confidentiality is important for this. Information security is therefore an integral part of privacy.

Information security is required in order to properly regulate privacy. That is why we see it as one subject: information security and privacy (IBP).

2 Purpose and scope

This policy has as goals:

- Ensuring the continuity of education and business management.
- Ensuring the privacy of pupils and employees, preventing security and privacy incidents and the possible consequences.

This policy is a guideline for everyone involved in IBP within the HSV. It applies to our own employees, temporary staff and other persons who play a role in the HSV. It applies to the entire organization including the physical locations, systems at internal and external locations and data collections that are used.

The information security and privacy policy has an interface with other policy areas, namely:

- General safety and security policy; with focus on company emergency services, physical access and security, crisis management, accommodation and accidents;

• IT policy; with the focus on the purchase and management of ICT;
• Personnel and organization policy; with areas of attention in and out of employees, segregation of duties and confidentiality positions;
This document makes clear where the responsibilities for information security and privacy are invested.

3 Principles

The most important policy principles at the HSV are:

- Information security and privacy must comply with all relevant laws and regulations
- The safe and reliable handling of information is the responsibility of everyone
- All employees, pupils, (registered) visitors and external relations are expected to behave 'decently' within their own responsibility
- The HSV is the legal entity for the information that is used under its responsibility
- The HSV makes concrete agreements with all parties with which personal data are exchanged about information security and privacy
- IBP is a continuous process, where it is regularly (at least annually) evaluated and it is checked whether adjustment is desired
- There is a balance between the risks of what we want to protect and the needed investments and measures
- There is a balance between privacy, functionality / workability and safety

3.1.1 Privacy

The HSV uses five rules for privacy:

1. Purpose and purpose limitation: personal data are only used for explicit and legitimate purposes. These purposes have been determined in concrete terms and prior to processing. Personal data are not processed further in a way that is incompatible with the purposes for which they were obtained.
2. Basis: processing of Personal Data is based on one of the legal bases: permission, agreement, law, public-law task, vital interest of the person concerned, or legitimate interest.
3. Data minimisation: when processing Personal Data, the quantity and type of data remain limited: the type of personal data must reasonably be required to achieve the goal; they are proportional to the target. The goal cannot be achieved with less, alternative or other data. This also means that data is not saved longer than necessary.
4. Transparency: the school gives notice in a transparent manner to those involved (pupils, their parents and employees) about the use of their personal data, as well as about the IBP policy. This information provision takes place unasked. In addition, these parties are entitled to the improvement, addition, removal or protection of their Personal Data. In addition, data subjects can oppose the use of their data.
5. Data integrity: measures have been taken to ensure that the Personal Data to be processed are correct and up-to-date

Personal data must be adequately secured according to general and widely accepted security standards.

For all registrations based on permission, the HSV will be offered an unambiguous so-called Opt-out procedure to the person concerned.

4 Laws and regulations

The HSV complies with all applicable relevant laws and regulations, including:

- Law on primary education
- Law good education and good governance PO / VO
- Law for the protection of personal information
- General Data Protection Regulation (AVG)
- Archive law
- Compulsory education law
- Copyright law
- Criminal law

Besides the provisions of the Covenant 'digital educational resources and privacy 2.0' leading in making agreements with suppliers

5 Organisation

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

- Leading (strategic)
- Steering (tactical)
- Executive (operational)

Roles, tasks and responsibilities are described for each level.

Leading
Final responsibility
The executive director is ultimately responsible for IBP and determines the policies and measures in the field of information security and privacy. The application and operation of the IBP policy is evaluated on the basis of regular reports. Within the schools, the school director is responsible for the IBP (IBP manager).

5.1.1 Steering

Manager IBP
Manager IBP is a role on steering level. He/she gives feedback and gives advice to the final responsible person and directs people. The IBP manager must:

- Translate the policy into guidelines, procedures, measures and documents for the entire institution
- Monitor the uniformity within the school
- Be the point of contact for incidents in the field of information security and privacy
- Coordinate the further handling of incidents within the school

Data Protection Officer

The data protection officer (FG) supervises the application and compliance with the privacy legislation within the HSV. The legal duties and powers of the FG give this official an independent position in the organisation. The FG handles confidential information security incidents. The FG is usually also the contact person for complaints and questions of those involved with a confidential character

5.1.2 In practice

Employees.
All employees have a responsibility with regard to information security in their daily activities. These responsibilities are described in the staff manual. In addition, employees are supported in their daily activities with checklists and forms where necessary.

Employees are asked to be actively involved in information security. This can be done by making reports of security incidents, making proposals for improvement and exercising influence on the policy (individually or via the GMR).

Supervisor
Compliance with the information security policy is part of the integral management. Each manager has the task to:

- ensure that employees are aware of the security policy;
- supervise compliance with the IBP policy by employees, in which he / she has an exemplary function;
- periodically highlight the subject of IBP in work meetings, assessments, etc .;
- be available as a point of contact for all staff-related IBP subjects.

The manager can be supported in his task by the data protection officer.

6 Control and reporting

This information security and privacy policy is reviewed and adjusted at least every two years. This takes into account:

-The status of the information security as a whole (policy, organization, risks)

-The effectiveness of the measures taken and their demonstrable effect

6.1.1 Information and awareness

Policies and measures are not sufficient to exclude risks in the field of information security and privacy. In practice, man is usually the most important player. That is why the awareness of the individual employees at the HSV is constantly tightened, so that the knowledge of risks is increased and safe and responsible behavior is encouraged. Increasing security awareness is a responsibility of the manager IBP.

6.1.2 Classification and risk analysis

The HSV information is valuable, therefore all data to which this policy applies is classified. The level of the 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. In addition, availability, integrity and confidentiality are the quality aspects that are important for the provision of information.

6.1.3 Incidents and data leaks

All incidents can be reported to the data protection officer. The handling of these incidents follows a structured process, which also provides for the correct steps regarding the obligation to report data leaks.

6.1.4 Control, compliance and sanctions

The Data Protection Officer (FG) plays an important role in promoting compliance with the Personal Data Protection Act. The FG is appointed by the executive director, and has a legally defined and independent supervisory role.

If the compliance is seriously inadequate, then the HSV can impose a sanction on the responsible employees involved, within the framework of the Collective Labor Agreement and the legal possibilities.

At HSV, the reporting of security incidents and data leaks is recorded in a protocol.