Stichting Primair en Voortgezet Onderwijs Zuid-Nederland

Information security and privacy policy

Datum instemming College van Bestuur	**26 maart 2018**
Datum instemming MR	**29 mei 2018**
Datum publicatie	**31 mei 2018**

Bron

saMBO-ICT
Kennisnet

Bewerkt door:

SPVOZN , M. Thiers - Controller

Vastgesteld door:

Versie	Datum	Naam
1.0	26 maart - 2018	College van bestuur

Translated:

This document is an English translation (by Davis International) of “Informatiebeveiligings- en privacy beleid”. In case of differences in interpretation between the English and Dutch versions of the policy, the original Dutch version shall prevail.

Content

1 The importance of information security and privacy

Education is increasingly dependent upon information and ICT. The amount of information, including personal data, is increasing because of, among other things, developments such as personalised learning with ICT. It is important to protect information and to handle personal data securely and responsibly. The dependency upon ICT and personal data carries with it new vulnerabilities and risks.

Regulating information security and privacy (IBP) properly in an IBP policy is necessary to reduce the consequences of these risks to an acceptable level and to be able to optimally ensure the progress of education and business management.

2 Explanation information security and privacy

2.1 Explanation information security

Information security encompasses taking and maintaining a number of coherent measures to ensure that the reliability of the provision of information can be guaranteed. Information security focuses on the following aspects:

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

Insufficient information security can lead to undesirable risks in the educational process and in the business management of the institution. Incidents in, and infringements of, these processes can lead to financial losses and image loss.

2.2 Explanation privacy

Privacy concerns personal data. Personal data have to be protected according to the current laws and regulations. Protection of the privacy regulates, among other things, the conditions under which personal data may be processed.

Personal data means all data that can identify a natural person directly or indirectly. Processing means every action with regard to personal data. The law mentions examples of such processing:

Collecting, entering, organizing, storing, editing, changing, requesting, consulting, using, supplying by means of forwarding, spreading or any other form of making information available, merging, connecting, screening, erasing and deleting of data.

2.3 Combination information security and privacy

From the aforementioned, it appears that information security is an important condition for privacy, while, the other way around, the careful handling of personal data is necessary for information security. Information security and privacy are equally important and dependent upon each other. They are, therefore, combined in one process: IBP. This policy – IBP policy – forms the basis of information security and privacy within Stichting Primair en Voortgezet Onderwijs Zuid-Nederland (SPVOZN) and forms the basis for the underlying agreements and procedures.

3 Purpose and scope

3.1 Purpose

Information security and privacy have the following purpose:

- Safeguarding the continuity of the education and business management.
- Guaranteeing the privacy of all those of whom SPVOZN processes personal data, including students, their parents/guardians and staff.
- Preventing security and privacy incidents and limiting the possible consequences.

The information and privacy policy (IBP policy) is focused on optimising the quality of the processing of information and security of personal data where the correct balance has to be found between privacy, functionality and security. The basis is that the personal life of the person concerned (a.o. staff, students and their parents/guardians) is respected and that SPVOZN satisfies relevant laws and regulations.

3.2 Scope

The IBP policy of SPVOZN applies to all staff, students, parents/guardians, (registered) visitors and external relations (contract / outsourcing). This policy also applies to all devices for which authorised access to the school network may be acquired.

The IBP policy applies to the processing of personal data of all those concerned in SPVOZN, including, in any event, all staff, students, parents/guardians, (registered) visitors and external relations (contract / outsourcing), as well as other persons concerned for whom SPVOZN processes personal data.

The policy applies to all those applications that fall under the responsibility of SPVOZN. This includes controlled information which has been generated and is managed by the school and the non-controlled information for which the school can be held responsible (i.e. statements of staff and students in discussions, on (personal pages of) websites and on social media).

The IBP policy applies to the entire or partly automated/systematic processing of personal data that takes place under the responsibility of SPVOZN, as well as the basic documents that are included in a file. The IBP policy also applies to non-automated processing of personal data that are included in a file or that are meant to be included.

In SPVOZN, IBP policy has links with:

- *General security and access security policy;* points for attention are in-house emergency services, physical access and security, crisis management, accommodation and accidents.
- *Staffing and organisational policy;* points for attention are joining and leaving of staff, changes in function, division of functions and confidential functions.
- *IT policy*; points for attention are purchase, management and use of ICT and (digital) learning resources.
- *Participation* of students, their parents/guardians and staff.

4 The policy – How do we draw this up?

SPVOZN uses the following starting points to reach the targets for information security and privacy:

1. The school board of SPVOZN accepts the responsibility to ensure that the information security and privacy is taken care of. The board may be held responsible and accountable. In terms of the law, the board is the responsible processing entity.

2. SPVOZN satisfies all relevant laws and regulations.

3. At SPVOZN, the processing of personal data is always linked to a specific purpose and based on one of the legal foundations. A proper balance between the interests of SPVOZN to process personal data and the interest of the person concerned to be able to make own choices with regard to the use of his/her personal data in a free environment is essential. With regard to all processing of personal data on the basis of permission, the persons concerned may revise their permission at any time.

4. SPVOZN will inform all those concerned in a clear and pro-active manner about the processing of their personal data, acquired directly as well as indirectly. The rights with regard to information, inspection, improving, erasing data, limiting processing, opposition, data portability and profiling.

5. SPVOZN registers all processing of personal data in a data register which will be kept up to date. SPVOZN complies hereby with the documentation duty.

6. At SPVOZN, safe and reliable dealing with information is everyone's responsibility, This does not only include active contributions to the safety of automated systems and the information stored but also of paper documents.

7. As legal entity SPVOZN is owner of the information that is produced under its responsibilty. In addition, the school manages information where the ownership (rights) belong to third parties. Staff and students are properly informed about the regulations with regard to the use of information.

8. SPVOZN classifies information and information systems. The classification is the basis for the risk analysis and the measures to be taken. There is a balance between the risks that should be covered and the necessary investments and measures to be taken.

9. SPVOZN enters into processing contracts with all suppliers of digital educational resources (educative as well as management applications) if they, commissioned by the school, process personal data. This also applies to other organisations if data of students and staff are supplied.

10. SPVOZN expects from all staff, students, (registered) visitors and external relations that they will behave in a 'proper' manner with an own responsibility. It is not acceptable that, as a result of behaviour wittingly or unwittingly, unsafe situations occur that lead to loss and/or loss of image. SPVOZN has formulated, determined and implemented a code of conduct in this respect.

11. At SPVOZN, information security and privacy is a continual process which is reviewed (at least annually) and assessed as to whether adjustments are necessary.

12. SPVOZN reviews the impact of changes in the infrastructure or the purchase of new (information)systems on the information security and privacy, in advance, so that the correct measures can be taken in a timely manner.

13. SPVOZN takes suitable technical (security) measures to protect personal data and other data from the risks that may affect the continuity of the education, the privacy and the business management.

14. SPVOZN will register all security incidents and data leaks in accordance with a fixed protocol and report them to the Authority Personal Data and, if necessary, to the persons concerned.

5 The policy in more detail – What do we do?

This chapter provides a practical content to the policy points above and is therefore the minimum content of the policy.

5.1 Relevant laws and regulations

The execution of the policy satisfies all applicable relevant laws and regulations, including:

- Law on primary education and/or Law on secondary education and/or Law on expertise centres
- Law on proper education and governance PO/VO
- Law inspection of education
- Law protection personal data (Wbp; up to 25 May 2018)
- General Regulation Data protection (AVG; from 25 May 2018)
- Archives law
- Educational law
- Authors law
- Penal Code

The international norm for information security NEN-ISO/IEC 27001 and 27002 (2015) is leading for the security measures to be taken.

The provisions of the most recent version of the covenant 'Digital educational resources and privacy' are leading in making agreements with suppliers that have been commissioned by the processing entity responsible to process personal data.

5.2 Basic rules in dealing with personal data

In processing personal data, the legal principles regarding processing personal data (art.5 AVG) are leading. These comprise **five basic rules** with regard to dealing with personal data, viz.:

1. **Reasons and binding purpose**: personal data are solely used for specifically described and justified purposes. These purposes are exact and determined in advance of processing. Personal data are not processed in a way that is incompatible with the purposes for which they are acquired.

2. **Basis**: processing of personal data is based on one of the six legal bases.

3. **Data minimalisation**: in processing of personal data the amount and type of data is limited: the type of personal data has to be, within reason, necessary to reach the target; they are in proportion to the target (proportional). The target cannot be reached with alternative or other data than is used (subsidiary). This also means that data is not stored longer than necessary.

4. **Transparency**: the school is accountable to those concerned (students, their parents and staff) in a transparent manner about the use of their personal data, as well as the IBP policy used. The provision of information takes place voluntarily. In addition, those concerned have a right to improvement, supplementation, deletion or screening of their personal data, as well as opposition from those concerned against the use of their data.

5. **Data integrity**: measures have been taken to safeguard that the personal data to be processed are correct and current.

5.3 Supporting guidelines and procedures

Various supplimentary policy papers, guidelines, procedures and protocols give content to the policy. Appendix 1 gives an overview of the various supplimentary policy papers, guidelines, procedures and protocols. In addition, all processes of personal data are registered and kept up to date in a data register.

5.4 Information and awareness

Policy and measures are not sufficent to exclude risks in the area of information security and privacy. The human factor is an important element. This is why the awareness of individual staff is continually heightened so that the knowledge of the risks is increased and safe and responsible behaviour is encouraged. Part of the policy is regularly recurring awareness campagnes for staff, students and guests.

Increasing the IBP awareness is a joint responsibility of IBP, the FG and the Security Officer, together with the board as entity with final responsibility.

5.5 Classification and risk analysis

All information has a value, which is why all data and information systems to which this policy applies, is classified. The level of the security measures to be taken is dependent upon the classification. The classification of the information is dependent on the data in the information system and is determined on the basis of risk analyses. Availability, integrity and confidentiality are the important reliability aspects.

In changes in the infrastructure or the purchase of new (information) systems, the impact of the developments and the intended processes on information security and privacy is determined in advance so that suitable measures can be taken. At the start of new (ICT) projects information security and privacy is taken into account.

5.6 Incidents and data leaks

All staff who suspect a security incident or data leak are required to report this. Reporting security incidents and data leaks is set out in a protocol. Dealing with these incidents follows a structured process that foresees in the correct steps with regard to duty to report data leaks. All (security) incidents may be reported to privacy@spvozn.nl.

Periodically, security incidents will be discussed and, where necessary, suitable policy measures will be taken.

5.7 Planning and control

This IBP policy will be reviewed at least every two years and, where necessary, amended by the board. The following will be taken into account:

- the status of the information security as a whole (policy, organisation, risks);
- the now known risks;
- the effectiveness of the measures taken and their demonstrable effect.

In addition, SPVOZN has an annual planning and control cycle for information security and privacy. This is a periodic evaluation process with which the content and effectiveness of the information security and privacy policy is tested. Any new developments in the area of technique, law and regulations, etc. are also taken into account.

5.8 Compliance and sanctions

Compliance consists of general supervision during daily practice on the adhering to policy and guidelines. It is important that the supervisors and process owners take their responsibilities and address their staff in cases of shortcomings. IBP is promoted within the institution, during performance interviews, in the broad code of conduct and with periodic awareness campagnes, etc.

In supervising compliance with the AVG, the Data Protection Officer (FG) fulfills an important role. The FG is appointed by the board and has a legally-defined and independent task. The FG works in accordance with regulations set by the board.

If compliance with this policy should fall seriously short, SPVOZN may sanction the staff responsible within the framework of the CAO (Collective Labour Agreement) and resort to the legal possibilities.

5.9 Logging and monitoring

Logging and monitoring by the IT department ensures that happenings with regard to automated systems and access to data is registered. This includes a.o. users logging in and out and (attempts to) unauthorised access to the network.

6 Organisation – Who does what?

6.1 Roles and responsibilities

The organisation of IBP deals with processes, habits, policy, laws and regulations that are important for the manner in which people steer, manage, direct and control an organisation. The relationships between the different people concerned and the targets of the organisation play a role. The overview below shows which responsibilities and tasks are part of which roles at SPVOZN:

Level	Who Roles	How Responsibility / tasks	What Realisation / registration
Directional (strategic)	Executive Board	• End responsibility • IBP policy making, registration and propogation • Responsibility for careful and legitimate processing of personal data • Evaluation of application and operation of IBP policy on the basis of reports • Organisation of IBP	• Information security and privacy policy • Baseline / basic measures • Determining regulations FG • Determining privacy regulations
Steering (tactical)	Manager IBP	• Responsible for the content of IBP • IBP planning and control • Advises CvB on IBP • Prepares execution IBP policy, Classification/risk analysis • Uses IBP norms and manner of testing • Evaluates IBP policy and measures • Translates general policy into specific policy in a uniform manner • Writes and manages processes, guidelines and procedures to support this execution	Processes, guidelines and procedures IBP, including: • Activity calendar • Protocol security incidents and data leaks • Organising processing agreements • Letter permission use of photos and videos • Drawing up information documentation for students, parents / guardians • Security awareness activities • Social media regulation • Code of conduct ICT and use of internet • Code of conduct of staff and students
	Data protection Officer / Privacy Officer	• Supervision compliance privacy legislation • Determination of guidelines, frameworks and making recommendations regarding improved protection of processing of personal data • Dealing with complaints and incidents	• Privacy regulation • Procedure dealing with IBP incidents • Organising contact point data leaks

Level	Who Roles	How Responsibility / tasks	What Realisation / registration
	Process owners including: ICT, staff, facility, education, finance, purchase and administration	• **Classification / risk analysis** *in cooperation with Manager IBP (Information manager / responsible IBP / Security officer).* • Determining access policy, physically as well as digitally and having it approved by *CvB.* • *Together with functional management and ICT management supervising that users only have access to the network and the network services for which they are specifically authorized*. • *Together with functional management and ICT management evaluating and checking the access rights of users regularly*.	• Making a list of what happens to personal data of the school (suppliers list). • Classification and risk analysis documents. Various supplimentary policy documents, guidelines, procedures and protocols, including: • Access matrix to various information systems and network
Operational (operational)	System manager Functional manager Member of staff Daily supervision / supervisor / director	• Dealing with incidents (registration and evaluation). • Technical point of contact for IBP incidents. • Executing tasks in accordance with specific guidelines and procedures. • Dealing responsibly with IBP in carrying out their daily work. • Communication to all those concerned; ensuring that staff is aware of the IBP policy and the consequences. • Supervision on compliance with the IBP policy and its processes, guidelines and procedures by the staff. • Setting an example with a positive and active attitude towards IBP policy. • Implementing IBP measures. • Periodically bringing the subject of information security to the attention in work meetings, performance interviews, etc. • Reporting progress to the board with regard to targets IBP policy.	Communication, information and supervision on compliance with a.o.: • IBP in general • Rules suitable education • How to deal with student files • Who are permitted to see what • Code of conduct • Dealing with social media • Making people media wise

More details about the roles and tasks may be found in appendix 2.

APPENDIX 1: Supporting guidelines and procedures

The appendix contains a number of supporting/supplementary policy documents, guidelines, procedures and protocols. A number are compulsory according to the General Regulation Data Protection (Algemene Verordening Gegevensbescherming).

	Documents:	**Points of attention:**
-	Procedure permission use of imagery	(letter of permission)
-	Procedure for the deletion of data	(storage periods)
-	Communication rights of persons concerned	(communication with the persons concerned)
-	Process description rights of persons concerned	(process with regard to applications from the persons concerned)
-	Privacy regulation	
-	Autorisation matrix	(who is permitted to view data, edit, etc.)
-	Agreements use of social media	
-	Procedure regarding staff training	(creating awareness)
-	Camera supervision	
-	Password policy	
-	Responsible disclosure	
-	Code of conduct use of ICT and internet	
-	Acceptable use policy	(responsible use of organisation resources)
-	Procedure regarding data exchange	(suitable education, student files, compulsory education, etc.)

The documents below are compulsory according to the AVG:

	Documents:	**Points of attention:**
-	Process description reporting data leaks	
-	Registration security incidents	
-	Data register to comply with registration duty	
-	Processing agreements	(making privacy appendix available)
-	Procedure data protection impact assessment	(DPIA)
-	Risk analysis	
-	Data protection officer	(communication with the staff on this subject)

APPENDIX 2: Organisation, who does what

This appendix describes how IBP is organisaed at three levels.

- Directional (strategic)
- Steering (tactical)
- Operational (operational)

To deal with information security and privacy in a structured and coordinated way at SPVOZN, for every level a number of roles are recognized which have been assigned to staff members in the existing organisation.
A description of the roles, the responsibilities and tasks can be found below, including the documents that relate to each role.

Directional

End responsibility
The Board has the end responsibility for IBP and determines the policy and basic measures in the areas of information protection and privacy.
The application and execution of the IBP policy is evaluated on the basis of regular reports. The responsibility for the content of IBP has been mandated to the manager IBP.

Steering

Manager IBP
Manager IBP is a role at steering level. He/she gives feedback and advice to the entity with end responsibility (the board) and manages people at executive level. The manager IBO is responsible for:

- Translating policy to guidelines, procedures, measures and documents for the whole institution.
- Safeguarding the uniformity within SPVOZN.
- Being the point of contact for incidents in the area of information security and privacy.
- Coordinating the handling of incidents within SPVOZN.

Data protection or Privacy Officer
The Data protection officer (FG) or Privacy Officer, if no FG has been appointed, supervises the application of and compliance with the AVG within SPVOZN. The legitimate tasks and authorities of the FB provide this officer with an independent position in the organisation. The FG ensures improvement and stimulation of awareness with regard to IBP, deals with information security incidents, advises on regulating privacy, maintains, if necessary, contact wth the Personal Data Authority (AP) and reports to the entity with end responsibility (the board). The FG regularly meets the manager IBP. The FG is also the point of contact for complaints and questions of persons concerned.

Process owners
Within the school, there are various domains/processes, such as ICT, staff (HRM, P&O), administration, facility management and financial matters, education, etc. For every one of these domains/processes, someone is responsible for determining in which manner IPB is utilized in guildelines, procedures and instructions.

These process owners are also responsible for the risks that are caused because people or applications gain illegitimate access to applications. To reduce these risks, process owners have the following specific tasks:

- Together with the entity with end responsibility, they determine policy for access (authorisations).
- Together with functional management and ICT management, they ensure that users only gain access to the network and network services for which they are specifically authorised and need access to for their work.
- Together with functional management and ICT management, they evaluate periodically the access rights of the users.

Operational

System manager
The Security Officer is the technical point of contact if it concerns information security for managemnt and staff..

Functional manager
Every software package or (web) application has a manager. For questions regarding software or application, it is known whom to contact. The functional manager is supplied by the process owner with a specific package of tasks, which include guidelines, procedures and instructions. On the basis of this package, he/she carries out his/her tasks.

Member of staff
All members of staff have a responsibility with regard to information security and privacy in their daily work. These responsibilities are described in the staff handbook and the manual acceptable use of resources of the organisation. In addition, if necessary, staff are supported in their daily work with checklists and forms.
Staff is asked to be actively involved in information security. This can be done by reporting security incidents, proposing improvements and by influencing policy (individually or via the MR).

Supervisor
Compliance with the information security policy is part of integral business management. Every supervisor has a task at executive level to:

- ensure that staff are aware of the IBP policy;
- supervise compliance with the IBP policy by staff in which he/she has to set an example;
- periodically draw attention to the subject IBP in work meetings, performance interviews, etc.;
- be available as point of contact for all staff-related IBP subjects.

The supervisor may be supported in his/her task by the manager IBP. Supervisors have to lead their staff by example.