RIJNLANDS INTERNATIONAL SCHOOLS THE NETHERLANDS

Rijnlands Lyceum

The International School Wassenaar
European School The Hague
International School of The Hague
International School Rijnlands Lyceum Oegstgeest

PRIVACY POLICY OF STICHTING HET RIJNLANDS LYCEUM

THE IMPORTANCE OF INFORMATION SECURITY AND PRIVACY

Education is increasingly dependent upon information and ICT. The amount of information, including personal data, is increasing due to developments such as personalised learning with ICT. It is important to protect information properly and to handle personal data securely and responsibly. Dependence upon ICT and personal data is accompanied by new vulnerabilities and risks. Proper regulation of *information security and privacy* (abbreviated to ISP) in an ISP policy is necessary in order to reduce the consequences of these risks to an acceptable level and to be able to optimally guarantee the progress of education and business operations.

Explanation of information security

Information security is understood to mean taking and maintaining a number of related measures so that the reliability of the information supply can be guaranteed.
Information security focuses on the following aspects:

- Availability: the extent to which data and/or functionalities are available at the right times.
- 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 restricted to those authorised for this.

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

Explanation of privacy

Privacy is about personal data. Personal data must be protected in accordance with current legislation and regulations. The protection of privacy covers, for example, the conditions under which personal data may be processed. Personal data in this context are all data that can directly or indirectly identify a natural person. Processing is understood to mean any act with regard to personal data. The law cites as examples of processing: *Collecting, recording, organising, storing, updating, modifying, retrieving, consulting, using, providing by means of transmission, distribution or any other form of provision, collating, linking, blocking, erasure and destruction of data.*

Interlinking of information security and privacy

From the above it appears that information security is an important condition for privacy, while, conversely, careful handling of personal data is essential for information security. Information security and privacy are linked and interdependent and are therefore combined into a single process: ISP. This policy, referred to below as

ISP policy, forms the basis for organising information security and privacy within Stichting Het Rijnlands Lyceum (the Stichting) and forms the basis for the underlying agreements and procedures.

Purpose

- Information security and privacy has the following objectives:
- Guaranteeing the continuity of education and business operations;
- Guaranteeing the privacy of all data subjects whose personal data the Stichting processes, including pupils/students, their parents/guardians and members of staff;
- Preventing security and privacy incidents and mitigating their possible consequences.

The information security and privacy policy (ISP policy) is aimed at optimising the quality of the processing of information and the security of personal data, while striking the right balance between privacy, functionality and security. The basic principle is that the privacy of the person concerned (including members of staff, pupils/students and their parents/guardians) are respected and that the Stichting complies with relevant legislation and regulations.

Scope

- The ISP policy within the Stichting applies to all members of staff, pupils/students, parents/guardians, (registered) visitors and external relations (hiring/outsourcing). This policy also covers all devices from which authorised access to the school network can be obtained.
- The ISP policy relates to the processing of personal data of all stakeholders within the Stichting, in any case including all members of staff, pupils/students, parents/guardians, (registered) visitors and external relations (hiring/outsourcing), as well as other stakeholders whose personal data is processed by the Stichting.
- The policy applies to those applications that are the responsibility of the Stichting. This includes audited information generated and managed by the school itself and unaudited information that the school can be held accountable for (e.g. statements made by members of staff and pupils/students in discussions, on (personal pages of) websites and/or social media).
- The ISP policy applies to the full or partial, automated/systematic processing of personal data performed under the responsibility of the Stichting as well as to the underlying documents held in a filing system. The ISP policy also applies to the non-automated processing of personal data contained in or intended to be contained in a filing system.
- Within the Stichting, ISP policy has points of contact with:
  - *General safety and access security policy*; with in-house emergency response, physical access and security, crisis management, accommodation and accidents as points of attention;
  - *Personnel and organisation policy*; with the focus on inflow and outflow of members of staff, job changes, segregation of duties and positions involving confidentiality;
  - *IT policy*; with the focus on the procurement, management and use of ICT and (digital) teaching materials;
  - *Participation* of pupils/students, their parents/guardians and members of staff.

Policy

The Stichting applies the following principles in order to achieve the objectives of information security and privacy:

1 The Executive Director of the Stichting is ultimately responsible for organising information security and privacy. The principal/director of the school has the delegated responsibility to ensure that information security and privacy is organised at his/her school. The principal/director is responsible and accountable for this. In terms of the law, the principal/director is the person responsible for processing. For the shared service centre, the Central Service Office, this is the ICT Manager.

2 The Stichting complies with all relevant legislation and regulations.

3 Within the Stichting, the processing of personal data is always linked to a specific purpose and based on one of the legal grounds. It is essential to maintain a good balance between the interest of the Stichting to process personal data and the interest of the data subject to make their own choices regarding the use of their personal data in a free environment. The parties involved may at any time reconsider their permission for the processing of personal data on the basis of consent.

4 The Stichting will inform all parties involved clearly and actively about the processing of their personal data, which has been obtained both directly and indirectly. All parties involved are also reminded of their rights with regard to information, access, rectification, erasure of data, restriction of processing, objection, data portability and profiling.

5 The Stichting records all processing of personal data in a data register and will keep this up-to-date. In doing so, the Stichting fulfils its obligation to provide documentation.

6 Within the Stichting, everyone is responsible for the safe and reliable handling of information. This not only includes actively contributing to the security of automated systems and the information stored within them, but also of paper documents.

7 The Stichting, as a legal entity, is the owner of the information produced under its responsibility. In addition, the school manages information, the ownership of which (copyright) belongs to third parties. Members of staff and pupils/students are properly informed about the regulations concerning the use of information.

8 The Stichting classifies information and information systems. The classification is the starting point for the risk analysis and the measures to be taken. There is a balance between the risks we want to hedge and the investments we need to make and the measures we need to take.

9 The Stichting concludes processing agreements with all suppliers of digital teaching materials (both educational and business applications) if they process personal data on behalf of the school. This also applies to other organisations if data concerning pupils/students or members of staff is provided.

10 The Stichting expects all members of staff, pupils/students, (registered) visitors and external relations to behave 'correctly' with respect to their own responsibility. It is unacceptable that intentional or unintentional behaviour should lead to unsafe situations leading to damage and/or loss of image. The Stichting has formulated, adopted and implemented an Integrity Code for this purpose.

11 Information security and privacy is a continuous process at the Stichting, with regular evaluations being performed (at least once a year) to determine whether adjustments are required.

12 In the event of changes to the infrastructure or the purchase of new (information) systems, the Stichting will examine the impact of these changes on information security and privacy in advance, so that the right measures can be taken in good time.

13 The Stichting will take appropriate technical (security) measures to protect personal data and other data against risks that may disrupt the progress of education, privacy and business operations. Optional: If the infrastructure is managed elsewhere and/or data is processed elsewhere, the Stichting

will make additional agreements about the technical measures.

14 The Stichting will record all security incidents and data leaks in accordance with a fixed protocol and report them to the Personal Data Protection Authority (*Autoriteit Persoonsgegevens*) and, if necessary, to the parties involved.

ELABORATION OF THE POLICY

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

Relevant legislation and regulations

The implementation of the policy complies with all applicable relevant legislation and regulations, including:

- Primary Education Act (*Wet op het primair onderwijs*) and/or Secondary Education Act (*Wet voortgezet onderwijs*) and/or Expertise Centres Act (*Wet op de expertisecentra*);
- Good Education, Good Governance Act (*Wet op Goed Onderwijs, Goed Bestuur*) primary/secondary education;
- Education Inspection Act (*Wet onderwijstoezicht*);
- Personal Data Protection Act (*Wet bescherming persoonsgegevens*) (until 25 May 2018);
- General Data Protection Regulation (*Algemene Verordening Gegevensbescherming*)(from 25 May 2018);
- Public Records Act (*Archiefwet*);
- Compulsory Education Act (*Leerplichtwet*);
- Copyright Act (*Auteurswet*);
- Penal Code (*Wetboek van Strafrecht*).

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

The provisions of the most recent version of the 'Digital teaching materials and privacy' covenant are the guiding principle when concluding agreements with suppliers who process personal data on behalf of the person responsible for processing.

Basic rules for handling personal data

The processing of personal data is governed by the statutory principles concerning the processing of personal data (Article 5 of the General Data Protection Regulation). These are summarised in the *five rules of thumb* relating to the handling of personal data:

1 *Goal definition and purpose limitation*: personal data will only be used for explicitly defined and legitimate purposes. These purposes have been specifically determined prior to the processing. Personal data will not be further processed in a manner incompatible with the purposes for which they were collected.

2 *Ground*: processing of personal data is based on one of the six legal grounds.

3 *Data minimisation*: the amount and type of data is limited when processing personal data: the type of

personal data must reasonably be required for the purpose; it must be proportionate to the purpose. The purpose cannot be achieved with less, alternative or different data (subsidiarity). This also means that data is not kept any longer than necessary.

4 *Transparency*: the school is accountable to the parties involved (pupils/students, their parents and members of staff) in a transparent manner for the use of their personal data, as well as for the ISP policy pursued. This information is provided on an unsolicited basis. In addition, the parties involved are entitled to have their personal data corrected, supplemented, deleted or blocked. The parties involved can also oppose the use of their data.

5 *Data integrity*: measures have been taken to ensure that the personal data to be processed is accurate and up-to-date.

Supporting guidelines and procedures

Various supplementary policy documents, guidelines, procedures and protocols substantiate the elaboration of the policy. In addition, all processing of personal data is recorded and kept up-to-date in a data register.

Information and awareness

Policies and measures are not sufficient to exclude risks in the area of information security and privacy. Human beings are an important factor in this respect. The awareness of individual members of staff is therefore constantly increased, so that the knowledge of risks is enhanced and safe and responsible behaviour is encouraged. Regular awareness-raising campaigns for members of staff, pupils/students and guests are part of the policy. Raising ISP awareness is a joint responsibility of the ICT Manager, the Data Protection Officer, the principals/directors and the management of the Stichting (executive director) as the person ultimately responsible.

Classification and risk analysis

All information has value, so all data and information systems to which this policy applies are classified. The level of security measures to be taken depends upon the classification. The classification of information depends upon the data in the information system and is determined on the basis of risk analyses. In this respect, availability, integrity and confidentiality are important aspects of reliability.
In the event of changes in the infrastructure or the purchase of new (information) systems, the impact of the developments and the intended processing on information security and privacy will be considered in advance, so that appropriate measures can be taken. Information security and privacy are taken into account from the start of new (ICT) projects.

Incidents and data leaks

All members of staff who suspect a security incident or data breach must report this. The reporting of security incidents and data leaks is laid down in a protocol. The handling of these incidents follows a structured process, which also provides for the correct steps to be taken with regard to the obligation to report data leaks. All (security) incidents are recorded in an incident register. All (security) incidents can be reported to the ICT employee responsible on site.
Security incidents will be discussed regularly and, where necessary, additional appropriate policy measures will be taken.

Planning and monitoring

This ISP policy will be reviewed and revised by the management of the Stichting at least every two years with account being taken of:

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

In addition, the Stichting has an annual planning and control cycle for information security and privacy. This is a regular evaluation process that assesses the content and effectiveness of the information security and privacy policy. It also takes account of current developments in the field of technology, legislation and regulations, etc.

Compliance and penalties

Compliance consists of general supervision in everyday practice of compliance with policy and guidelines. It is important in this respect that managers and process owners assume their responsibility and hold their members of staff to account in the event of shortcomings. Active attention is paid to ISP when appointing members of staff, during performance reviews, with an institution-wide code of conduct, with regular awareness-raising campaigns, etc.
The Data Protection Officer plays an important role in supervising compliance with the General Data Protection Regulation. The Data Protection Officer is appointed by the Stichting and has a legally defined and independent supervisory role. The Data Protection Officer verifies the ISP regulations to be drawn up by the Stichting.

Should compliance with this policy seriously fail, the Stichting may impose a sanction on the responsible members of staff involved, within the framework of the collective labour agreement and the legal possibilities.

Logging and monitoring

Logging and monitoring by the ICT manager ensures that events relating to automated systems and access to data are recorded. This includes, for example, the logging in of users and (attempts) to gain unauthorised access to the network.