Stichting Primair en Voortgezet Onderwijs Zuid-Nederland

Code of Conduct for Responsible Use of ICT and Internet

Datum instemming College van Bestuur	**4 juni 2018**
Datum instemming MR	**24 oktober 2018**
Datum publicatie	**25 oktober 2018**

Bron

Kennisnet

Bewerkt door:

SPVOZN , M. Thiers - Controller

Vastgesteld door:

Versie	Datum	Naam	Functie
1.0	4 juni 2018	M. Stoker	Voorzitter College van Bestuur

Bijgewerkt :

Datum	Naam	Functie	Aanpassing

Translated:

This document is an English translation (by Davis International) of “Gedragscode voor verantwoord gebruik van ICT en internet”. In case of differences in interpretation between the English and Dutch versions of the regulation, the original Dutch version shall prevail.

CONTENT

1 Introduction

The use of internet, computer and email is necesary for all staff of the school to be able to carry out their work. For these activities, use is made of large amounts of data, including personal data. The (ICT) facilities and the different types of data are called ‘organisation resources’ in this document. These organisation resources include:

- Hardware: computer, laptop, tablet,… telephone,
- Software: all applications, programs, apps, mobile or not, that are used for carrying out the work activities, such as the email environment, Microsoft Office, Student and Staff administrative systems and digital lesson materials, Electronic learning environments and so on. Also take into consideration, Google and other cloud services.
- Information and (personal) data: reports, student files, data in emails. In this regard, arising from the privacy legislation, the processing of personal data requires additional measures.
- Use of internet: visiting website, the use of email and other online services, but certainly also the social media, such as Facebook, LinkedIn, Instagram and Twitter.

There are risks involved in the use of ICT and internet, which make it necessary to make agreements about their use. It is expected of staff of SPVOZN that they use the available organisation resources responsibly. This is also expected when staff use their own resources to carry out work for the school.

The agreements in this document apply to all locations from which (school) activities are carried out. They apply to everyone who works for SPVOZN itself or through external organisations commissioned by SPVOZN, including trainees, LIO and temporary staff as well as employees in the service of the Consortium working on the ISE.

1.1 Bases for code of conduct

This code of conduct sets out the rules for the use of ICT and internet by staff and the control on compliance.
The purpose of this code of conduct is to set out the norms and bases regarding:

- system and network security, including security against damage and misuse
- the protection of privacy-sensitive information, including personal data of the school board, its staff, students and their parents for the protection of the privacy and safety of all those concerned
- the protection of confidential information of the school board, its staff, students and their parents
- preventing and counteracting misuse of ICT and internet
- the protection of the intellectual property rights of the school board and third parties
- avoiding negative publicity
- control on costs and capacity.

The control on the use of ICT and internet is a processing of personal data in the sense of the privacy legislation. SPVOZN will execute the control and enforcement of these rules in accordance with the privacy legislation and the framework of general employment laws. The basis for this is a good balance between responsible use of ICT and internet and the protection of the privacy of staff at the workplace. Data is solely collected and used for these purposes. In particular, the board will secure the data stored by control against unauthorised access. The board will enforce contractually sufficient confidentiality from persons with access.

1.2 Own responsibility and private use

The use of the organisation resources supplied by SPVOZN is personal and remains the responsibility of the member of staff. All devices that are used for school work (including ‘own devices’) will not be loaned out or made available to others without additional (security) measures. Non-compliance with the rules for information security and privacy could lead to disciplinary measures.

1.3 Various types of data

SPVOZN is responsible for setting up and organising information security and privacy. The main purpose of the information security and privacy is the protection of data.
SPVOZN makes a distinction between three types of data:

- Public data; this is data meant for publication.
- Internal data; this is data for exclusive use and processing within SPVOZN. Think before sharing this data with external parties.
- Confidential data; this is data exclusively accessible to specific, authorised staff within SPVOZN. These could be (special) personal data, staff data or tender data.

Personal data deserve special attention. This is data that concerns a person and by which a person is identified or identifiable. This could be name data, email addresses but also telephone number of colleagues as well as students and parents of students.

The privacy legislation obliges every individual to handle personal data carefully. One part of the legal obligation is that SPVOZN has to have written agreements with suppliers of (online) applications, whereby personal data is processed (this could be login data, passwords and storage of work).

SPVOZN has appointed Orion as Data Protection Officer. This company supervises application and compliance with the AVG within our foundation.

If personal data are accessible or can be viewed by persons who should not have access to these data, a security incident has occurred from which a possible data leak may arise. Such an incident can have harmful consequences for the person(s) concerned and SPVOZN.
In order to handle this data in a safe, responsible and workable manner, SPVOZN has agreed the following:

- the processing and distribution of confidential and personal data. Only data that are necessary to reach the required objectives are processed.
- The exchange of data whereby the receiver is informed what the receiver may or may not do with the data.
- Storage and distribution of data, whereby exclusive use is made of organisation resources approved by SPVOZN.

It is expected of staff of SPVOZN and/or external staff, who have access to the digital information systems and have access to, for instance, staff files, confidential questionnaire data, care files, etc, that they handle the information made available to them due to their function with care. That they comply with the privacy legislation and, in no way, use and/or make public any information from which can be reasonably assumed to be privacy sensitive without permission of the person involved or the supervisor.

2 Code of Conduct

In this code of conduct for responsible use of ICT and internet, SPVOZN sets out the agreements with regard to the different subjects surrounding the use of ICT and internet and what this means to staff in daily practice.

2.1 General standards

Every member of staff should meet the following general norms for 'care' (not complete):

- Handle personal data carefully, whereby knowledge of the basic rules for handling personal data is expected.
- Prevent leaks of internal and confidential information.
- Ensure good physical and technical protection of organisation resources (security measures). (beveiligingsmaatregelen).
- Prevent deliberate bypassing of security measures (for instance by jailbreaks).
- Report theft or loss of organisation resources immediately by sending an email to **privacy@spvozn.nl** or by reporting it by telephone to the designated person (see procedure duty to report data leaks of SPVOZN).

2.2 Computer use

In order to carry out their work, SPVOZN provides members of staff with computer and network facilities (organisation resources). The use of these organisation resources is connected to these activities and assumes the following agreements:

- Ensure that privacy-sensitive data is not accessible to unauthorised persons.
- Be aware of which data may be used (is everyone allowed to see it?) and which ICT facilities may be used (is it safe enough?) in carrying out the various school activities.
- Store (personal) data only on the designated systems. (Storing (personal) data in public Cloud environments, such as a personal Dropbox, is not permitted).
- Encrypt all data with regard to SPVOZN, in the event that this data, for whatever reason, is stored elsewhere (this includes a usb stick).
- Never share passwords, not even on occasion. Passwords are personal.
- Lock the pc, when temporarily leaving the workplace (windows key +L).
- Close off the computer after use or log out.
- Report malfunctions of controlled workplaces (computer or laptop) to the ICT department through Topdesk.

2.3 Workplace

Prevent that others unintentionally can gain access to organisation resources to which they are not entitled and/or do not unintentionally leak data. As additional rules on computer use for workplaces, the following clean-desk and clear-screen rules apply:

- Lock the pc when temporarily leaving the workplace (windows key+L).
- Remove internal and confidential documents from the desk when leaving the workplace for a longer period (such as attending a meeting).
- Prevent visibility of sensitive and confidential information when someone else can see the screen (or through a beamer). Close the email program and maintain a clean digital desktop.
- Do not leave prints at the printer, in particular with personal data.
- Always put superfluous paper documents with personal data through the paper shredder.

ATTENTION: If personal data is accessible/visible to persons who should not have access to this data, a security incident has occurred from which possibly a data leak could arise. Be aware that security incidents and possible data leaks should be reported in accordance with the SPVOZN procedure duty to report data leaks.

2.4 Use of own devices (BYOD)

Security measures apply to all devices with which activities for SPVOZN are carried out. SPVOZN is responsible for the implementation of the correct security measures when it involves organisation resources of the school.

For ‘own devices’ the responsibility for adequate security measures lies with the member of staff. The member of staff is expected to have minimally taken the following security measures:

- Secure the device with a password, or in the case of a smartphone or tablet, with a pincode of at least 4 digits.
- Lock the device when leaving the workplace (windows key+L).
- Do not store personal data of SPVOZN on the own device; this is not permitted.
- Encrypt all data, other than personal data, with regard to SPVOZN if this, for whatever reason, is not stored on the school network (including own device or usb stick).
- Separate (encrypted) data, other than personal data, of SPVOZN from private data. This separation has to be clearly recognizable on the own device.
- Keep software up to date by carrying out periodic updates (at least monthly).
- Take adequate measures against virusses or malware by keeping the virusscanner up to date and by periodically (at least monthly) scanning the device.

SPVOZN is permitted to carry out checks on the measures mentioned above. At the request of SPVOZN, the member of staff is required to demonstrate that the above-mentioned measures are being applied.

2.5 Software and digital lesson materials

The use of digital lesson materials is common practice at SPVOZN. This lesson material is more and more available online by which personal data is exchanged more and more frequently. The privacy legislation demands that every organisation reviews in advance the influence on the privacy by the use of such material. This can lead to specific measures.
The rules below apply to the installation and use of software and (online) digital lesson materials:

- Installation of software is only permitted by SPVOZN with the correction licenses and after taking any additional measures.
- When using online software, apps and digital lesson materials, any use of personal data is reviewed.
- A processing agreement is entered into with every supplier of (online) software who processes personal data under commission of SPVOZN.
- There is an agreed application procedure for digital lesson materials and/or other software at SPVOZN. Any application should be made through TOPdesk.

2.6 Use of email

SPVOZN provides the member of staff with an email system and corresponding mailbox to carry out the activities. Use of email facilities is connected to these activities and assumes the following agreements:

- Use the school email address exclusively for school-related matters.
- For the use of private email, use an external webmail service and a private email address (for instance webmail of Gmail, Hotmail or an own provider).
- Receipt of private mail at the school email address is permitted incidentally.
- The sending of email should meet the normal codes of conduct that apply to written correspondence.
- It is not permitted to use email for messages with pornographic, racist, discriminatory, insulting (sexually) intimidating or offensive content or for messages that could encourage hate and violence.
- If a member of staff synchronises school email with own devices (tablet, telephone), in the event of loss or theft of the device, SPVOZN may use the possibility to wipe the email remotely, even if this means that all (private) data will also be deleted.

2.7 Use of internet

SPVOZN provides the member of staff with the use of internet and corresponding facilities for execution of the activities. Use is connected to these activities and assumes the following agreements:

- Limited personal use is permitted, if this
  - o does not interfere with the daily activities
  - o is not for commercial purposes and does not result in forbidden use.
- It is not permitted to
  - o visit sites on the internet that contain pornographic, racist, discriminatory, insulting or offensive material
  - o download films, music, software and other copyright protected material from an illegal source
  - o use internet access for private reasons during lesson times
  - o participate in gaming.
- It is forbidden to communicate through online forums, social networks and other comparable communication networks in a threatening, insulting, sexually-tinted, racist or discriminatory manner regarding all those connected to the school and school activities. This applies in particular also to internet use outside the school network with regard to those connected to the school and school activities.

2.8 Online safety

Together, we spend more and more time online. More and more often mobile devices are used. Human (online) actions are often the basis of a data leak.
SPVOZN expects of its members of staff that they:

- Are able to distinguish between secure and unsecured networks (public wifi)
- Safe and unsafe websites (safe websites have a little lock)
- When processing personal data only use familiar and secured wireless networks
- Are aware what malware is, are able to recognise it and know how to handle it and are restrained in leaving data online with regard to SPVOZN
- Check whether use is being made of a familiar and secured network when visiting public spaces.

2.9 Social media

Social media is a collective name for all internet applications that make it possible to share information together in a simple and often fun manner. It does not only concern information in the form of text (news, articles). Sound (podcasts, music) and images (photography, videos) are shared through social media (Instagram, YouTube, Facebook, Twitter enz). The essence of social media is that someone shares information about him/herself, about others or about a particular subject.
The basis for the use of social media is that the digital behaviour on social media should not deviate from the real life behaviour within the school. Members of staff are always the representatives of SPVOZN, even if they express a private opinon online.
For SPVOZN, the following agreements for the use of social media apply:

- Share knowledge in a responsible way through social media, taking the good name of SPVOZN into account and everyone concerned.
- Make it clear with education-related subjects whether publication is personal or on behalf of SPVOZN.
- Do not publish confidential information on social media.
- Do not publish images of students without the express prior explicit permission of parents, if the student is younger than 16 years old, or of the student, if the student is 16 years of age or older.
- Be aware that publications on social media can always be traced (public) and are difficult to delete/destroy. Members of staff are personally responsible for what they publish.
- Contact a superior if there is any doubt about a publication or about connection to SPVOZN.
- It is not permitted for staff to be ‘friends’ with students and parents on social media.
- Use of social media in the lesson programme is bound by the permission of parents if students are younger than 16 years of age.

2.10 Use of image and sound materials

The use of image and sound materials, the sharing of photos, videos and sound fragments of students by staff under the responsibility of SPVOZN is only permitted if prior permission has been given by parents, if the student is younger than 16 years old, or by the student, if the student is 16 years of age or older. Without this permission, no fotos, videos and sound fragments of students may be used.

- SPVOZN refers to the guidelines that have been drawn up for the use and permission of images.
- For the agreements concerning the sharing of images and sound materials on social media, the guidelines, which are listed for the use of social media, apply.

2.11 Passwords and pincodes

Securing access to the network, various (online) applications and devices (pc, laptop, telephone) starts with a good password. A long password or a ‘pass sentence’ is better than a short, complex password. For the use of passwords, the following agreements apply:

- Passwords should have a minimum of 8 characters, with at least three of the following four elements: small letter, capital letter, number or special symbol (!@#$%^&*()
- Pincodes (on telephone or tablet) should be longer than 4 digits.
- Passwords should be replaced from time to time, in accordance with agreements within SPVOZN.
- Do not use the same password for every system.
- Never share passwords, not even on occasion. Passwords are personal.

2.12 Duty to report data leaks

It is expected of all members of staff that they report security incidents and possible data leaks in accordance with the procedure duty to report data leaks of SPVOZN (via privacy@spvozn.nl).

3 Control on use of ICT and internet

SPVOZN acts in accordance with the current laws and regulations in the control on the use of ICT and internet, e.g.:

- The Constitution,
- Law on the protection of personal data - Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018),
- General Regulation Data Protection - Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018),
- Law Participation in Education - Wet Medezeggenschap Onderwijs (WMO),
- The Civil Code - Burgerlijk Wetboek (BW),
- Criminal Law - Wetboek van Strafrecht,
- Labour Agreement Primary Education - Cao PO and
- Labour Agreement Secondary Education - Cao VO.

SPVOZN will assume the correct balance between responsible use of ICT and internet and the protection of the privacy of staff in control of the use of ICT and internet on the basis of this code of conduct.

3.1 Conditions for control

- Control of personal data with regard to use of ICT and internet will only take place in the context of maintaining the purpose of this code of conduct.
- Control will in principle take place on the level of totalised data that cannot be traced to identifiable persons.
- If a member of staff or a group of members of staff are suspected of breaking the rules, a targeted control may take place, commissioned by SPVOZN, during a set (short) period.
- Control is in principle limited to data traffic of the email and internet use. Only for important reasons will a control on content take place, commissioned by SPVOZN.
- Forbidden email and internet use will be made impossible as much as possible by software.
- When unauthorised use is noticed, this will be discussed immediately with the member of staff concerned. The member of staff will be informed of the consequences if unauthorised use is not stopped.
- If the member of staff disagrees with the proposed disciplinary measure, then, in a number of cases, an objection and/or appeal can be made (see 3.4).
- Email messages of members of the MR, the confidential persons, company doctors and of anyone who, on the grounds of function, must be able to rely on confidentiality, are not controlled in principle. However, this can be deviated from, for important reasons.

3.2 Carrying out the control

- The control in order to avoid negative publicity and sexual intimidation and the control in the context of system and network security takes place on the basis of content filtering.
- The control on leaks of internal and confidential information takes place on the basis of random testing content filtering. Suspicious messages will be isolated for further investigation.
- The control in the context of costs and capacity control is limited to traffic and storage data.
- Control on the use of image materials takes place on the basis of complaints or notifications from third parties, or random testing of image materials that is publically available.
- The ICT department is bound by confidentiality if, for technical reasons, it is necessary to acquire personal information, except when there are legal requirements for communication or the necessity for communication stems from the tasks.
- SPVOZN will take to necessary measures to ensure that personal data, in view of the purposes for which they are processed, are correct and accurate.
- SPVOZN will take suitable technical and organisational measures to secure personal data against loss and/or any form of illegal processing.

3.3 Disciplinary measures in the context of the code of conduct

In the event of not acting in accordance with this code of conduct or the generally applicable legal regulations, the board of SPVOZN, depending on the nature and seriousness of the violation, may take disciplinary measures. These include a warning/reprimand, compensation, making a police statement, transfer, suspension and/or termination of the contract of employment.
Staff that do not adhere to the code of conduct, will be approached by their supervisor as soon as possible to discuss their behaviour. They will be allowed to view the recorded data on them and given the opportunity to react to it. Member of staff and supervisor then make agreements for the future and determine the possible measures in the event of violation. These agreements may be stricter than those in the code of conduct. The access to email or internet may be limited or completely cut off.
Disciplinary measures (except a warning) may not be taken exclusively on the basis of an automatically executed processing of personal data, such as finding an automatic filter or blockage.
No disciplinary measures are taken before the member of staff has had the opportunity to express a point of view.

3.4 Objection and appeal

If a member of staff does not agree with the (proposed) disciplinary measure, in a number of cases, an objection and/or appeal may be launched. This is usually set out in the contract of employment, regulations regarding personnel matters and/or the applicable labour agreement.

4 MR (Participation Council)

This document refers to the processing of personal data and/or control on the behaviour or performance of members of staff. The participation council (the MR), for this reason, has to give consent. This council agreed with the content of this code of conduct on 24 October 2018.

The organisation may change this code of conduct, with the approval of the MR, if the circumstances give rise to this. Proposed changes will be announced to the members of staff prior to implementation.

5 Concluding clause

This regulation will be reviewed annually by SPVOZN and the MR.
The next review will take place in 2019.