**TOESTELBELEID**

**Vzw KobaHeli**BE 0448.528.592 Nooitrust 42390 Malle

voor:

**Basisschool Het Spoor**

**Instellingsnummer** 9662

Spoorweglei 6 Lier

***Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB).***

O

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versie** | **Datum** | **Status** | **Auteur(s)** | **Opmerking** |
| 1.0 | 2018-05-26 | GELDIG | VZW KOR Lier |  |
| 2.0 | 5 april 2021 | GELDIG | VZW KobaHeli | VZW aangepast |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Inleiding

|  |  |
| --- | --- |
| 1.1 AlgemeenIn een eenvoudige interpretatie zijn er drie aspecten van een modern ICT-netwerk om rekening mee te houden inzake beschikbaarheid, integriteit en vertrouwelijkheid:* **(Eind)gebruikers** = *personen*
* **Toestellen** = *desktops, laptops, maar ook tablets, smart-phones, … en ook: servers*
* **Netwerk(en)** = *de verbinding(en) tussen gebruikers en toestellen*
 |  |

In deze nota wil basisschool Het Spoor enerzijds regels bepalen om de bijdrage van elk van deze drie aspecten in het IVP-beleid te maximaliseren, en anderzijds wordt toegelicht hoe op basisschool Het Spoor **controle** op elk van deze aspecten gevoerd wordt.

Deze nota valt onder de eindverantwoordelijkheid van VZW KobaHeli Malle.

## 1.2 Algemene bepalingen

Ongeacht het “type” toestel of netwerk, zijn er een aantal maatregelen die basisschool Het Spoor steeds toepast. Hieronder worden deze opgesomd. In wat volgt, worden de specifieke maatregelen toegelicht.

# Netwerkbeveiliging en -controle

## 2.1 Bekabeld netwerk en servers

Met het “bekabelde netwerk” bedoelen we het geheel van componenten die de netwerkverbindingen maken en beheren, zoals: routers, switchen, hubs, kabels, modems, …

Wachtwoorden op de netwerkcomponenten worden systematisch gewijzigd t.o.v. de “default” waarden, of te gemakkelijke combinaties. De gekozen wachtwoorden voldoen i.h.b. aan alle afspraken uit het ***wachtwoordbeleid***.

## 2.2 Wifi-netwerk

Voor personeel, leerlingen en gasten is wifi voorzien op basisschool Het Spoor . Deze dienst is gratis voor de eindgebruikers, maar heeft voor de school wel een zekere kostprijs (in aanschaf, onderhoud en beveiliging).

De algemene maatregelen (zie § 1.2) worden toegepast, met i.h.b. logging van: MAC- en IP-adressen, toestelnamen, gebruikersnamen.

Het netwerkverkeer dat via het draadloze netwerk verloopt, wordt *niet* versleuteld. Het raadplegen, bewerken enz. van persoonsgegevens wordt dan ook ten stelligste afgeraden, tenzij er een andere vorm van versleuteling gehanteerd wordt (*bv. https i.p.v. http*).

# Beveiliging en controle op internetverkeer

Op basisschool Het Spoor is er, zowel voor de toestellen die eigendom zijn van de school als op bepaalde andere toestellen (zie ook § 2.2, § 4 en § 5), een internetverbinding mogelijk.

Als organisatie is basisschool Het Spoor verantwoordelijk voor het algehele dataverbruik, en voor alles dat er met / via deze internetverbinding gebeurt.

De beheerders, noch de elektronische controlesystemen, hebben op geen enkele manier toegang tot de inhoud van persoonlijke berichten (zoals messaging, email, intern communicatiesysteem, …).

# Beveiliging en controle op toestellen van de school

Onder “toestellen” van de school rekenen we zowel desktop computers, laptops, tablets die eigendom zijn van de school.

## 4.1 Algemeen

De volgende beveiligingsregels resp. -controles kunnen hierop (tegelijkertijd) toegepast worden:

* De beheerders steken veel tijd en geld in het zo vlot mogelijk “draaiend” houden van alle hardware en het netwerk. Dit is onmogelijk als gebruikers de systeem- of beveiligingsinstellingen veranderen. Er worden op basisschool Het Spoor dan ook verschillende maatregelen genomen om dit te verhinderen. Het doelbewust veranderen van systeem- of beveiligingsinstellingen is verboden.
* Leerkrachten en ondersteunend personeel kunnen, in het kader van hun uit te oefenen taak, de actieve ven-sters, geopende websites en/of het beeldscherm zien. Het is niet uitgesloten dat de inhoud van **persoonlijke berichten** (ontvangen en/of verzonden) leesbaar is, alhoewel dit nooit het doel op zich zal zijn. Al deze mede-werkers behandelen de informatie strikt vertrouwelijk, en bewaren deze niet.
* Het is, met dezelfde tools, wel toegestaan dat de beheerders, directie en eventueel andere personeelsleden die hiervoor bevoegd geacht worden, de schermen bewaren (als een schermafdruk of als een opname). Zij doen dit enkel bij een concreet vermoeden van doelbewuste en ernstige inbreuken en alle informatie wordt strikt vertrouwelijk behandeld. Onbevoegde medewerkers hebben geen toegang tot de schermafdrukken of opnames.

## 4.2 Vergrendeling, encryptie en wissen van op afstand

De mobiele toestellen (d.w.z. laptops, tablets, smartphones) die bepaalde personeelsleden gebruiken maar die eigendom zijn van basisschool Het Spoor , dienen extra beveiligd te worden indien er persoonsgegevens op bewaard, bekeken of verwerkt worden.

I.h.b. wordt er een vergrendeling a.d.h.v. wachtwoord, pincode, swipe code, vingerafdruk of andere authenticatie toegepast.

Voor directie, ondersteunend personeel dat toegang heeft tot gevoelige persoonsgegevens op het toestel in kwestie, zorgverantwoordelijken en CLB geldt bovendien:

* Optie om te lokaliseren of te wissen van op afstand, in geval van diefstal of verlies (indien mogelijk)

# Beveiliging en controle op toestellen van eindgebruikers zelf

Op basisschool Het Spoor is het mogelijk om, via het netwerk of wifi van de school (zie ook § 2), gebruik te maken van eigen toestellen. Het is de bedoeling dat deze maximaal gebruikt worden om taken uit te voeren, gerelateerd aan de onderwijsinstelling.

## 5.1 Algemeen

Inzake een eigen toestel zijn een aantal beveiligings- en beheerdersaspecten anders dan in § 4. Desalniettemin gelden alle principes van deze paragraaf evenzeer voor handelingen gerelateerd aan basisschool Het Spoor , die uitgevoerd worden op een eigen toestel. Zie, naast § 4 uit deze nota, ook het algemene ***communicatiebeleid***. De bijzondere regels en afspraken inzake het BYOD[[1]](#footnote-2)-beleid, zijn:

Het internetverkeer en gebruikte toepassingen wordt, op verscheidene niveau’s, gecontroleerd inzake capaciteit maar ook veiligheid van de toepassing, het al dan niet veranderen van systeeminstellingen (gerelateerd aan beveiliging resp. prestaties, enz.)

De algemene maatregelen (zie § 1.2) worden toegepast, met i.h.b. logging van: MAC- en IP-adressen, gebruikersnamen, toestelnamen, gebruikte toepassingen, wijzigingen in systeeminstellingen, enz.

## 5.2 Vergrendeling, encryptie, antivirusbeveiliging, backups en wissen van op afstand

De mobiele toestellen (d.w.z. laptops, tablets, smartphones) van medewerkers, waarop persoonsgegevens van basisschool Het Spoor bewaard, bekeken of verwerkt worden, dienen extra beveiligd te worden. Dit beleid vraagt die medewerkers dan ook om de volgende maatregelen op deze toestellen in acht te nemen:

* Er wordt een vergrendeling a.d.h.v. wachtwoord, pincode, swipe code, vingerafdruk of andere authenticatie gevraagd.
* Er wordt gevraagd om een ten allen tijde up-to-date antivirusprogramma te gebruiken.
* Backups dienen genomen, bewaard en beheerd te worden zoals in het respectievelijke beleid vastgelegd.

Voor directie, ondersteunend personeel dat toegang heeft tot gevoelige persoonsgegevens op het toestel in kwestie, zorgverantwoordelijken en CLB wordt daarenboven het volgende gevraagd:

* Optie om te lokaliseren of te wissen van op afstand, in geval van diefstal of verlies (indien mogelijk)



1. BYOD = “bring your own device”. Het gebruik van eigen toestellen op en voor schoolgerelateerde processen. [↑](#footnote-ref-2)