TOESTELBELEID

vzw VRIJ KATHOLIEK BASISONDERWIJS DE WEGWIJZER

voor:

VRIJ KATHOLIEK BASISONDERWIJS DE WEGWIJZER bestaande uit de scholen:

- **VBS Beveren-Leie**
- **VBS Biest-Jager**
- **VBS Desselgem**
- **VBS Duizend+Poot**
- **VBS Gaverke-College**
- **VBS Keukeldam – Sint-Petrus**
- **VBS Nieuwenhove**
- **VBS Zulte**

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

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2019-01-22	GELDIG	CIV	

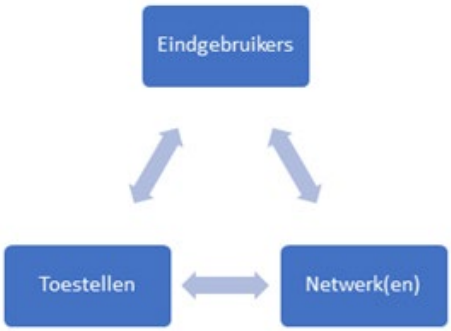
Inhoud

1. INLEIDING

1.1. Algemeen

In 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, smartphones, … en ook: servers
- **Netwerk(en)** = de verbinding(en) tussen gebruikers en toestellen



In deze nota wil Vrij Katholiek Basisonderwijs De Wegwijzer enerzijds regels bepalen om de bijdrage van elk van deze drie aspecten in het IVP-beleid te maximaliseren, en anderzijds wordt toegelicht hoe op Vrij Katholiek Basisonderwijs De Wegwijzer controle op elk van deze aspecten gevoerd wordt.

Deze nota valt onder de eindverantwoordelijkheid van vzw Vrij Katholiek Basisonderwijs De Wegwijzer.

1.2. Algemene bepalingen

Ongeacht het “type” toestel of netwerk, zijn er een aantal maatregelen die Vrij Katholiek Basisonderwijs De Wegwijzer steeds toepast. Hieronder worden deze opgesomd. In wat volgt, worden de specifieke maatregelen toegelicht.

- Het voorzien van manieren om te herkennen wanneer het “gewone” verkeer gemonitord, onderschept, nagebootst of gewijzigd wordt.
- Het combineren met een aantal monitoring tools en/of logboeken, d.w.z. manieren om de handelingen bij te houden voor analyse of eventueel naar bewijslast toe.
- In deze logboeken worden een aantal **identificatieparameters** geregistreerd. Er vinden geen ongeoorloofde inzagen of systematische analyses plaats op deze gegevens. Enkel bij gegronde vermoedens van inbreuken kunnen hierop gerichte en/of willekeurige controles uitgevoerd worden. Alle informatie hier aangaande wordt strikt vertrouwelijk behandeld.
- Een netwerk functionerend houden vereist toezicht en controles (≠ alles volgen wat een leerkracht doet). Deze controles gebeuren in het algemeen. Enkel in geval van (aanhoudende) problemen (bijv. overbelasting van het netwerk) kan het toezicht/de controle gericht worden en wordt er, indien nodig, overleg gepleegd met het betrokken personeelslid. Dit gebeurt door de directeur.

2. NETWERKBEVEILIGING & - 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, servers, modems, …

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

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 en gasten is WiFi voorzien op Vrij Katholiek Basisonderwijs De Wegwijzer. Deze dienst is gratis voor de eindgebruikers, maar heeft voor de school wel een zekere kostprijs (in aanschaf, onderhoud en beveiliging).

Daarom wordt de aard en hoeveelheid van het netwerkverkeer gemonitord.

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

Ook de bezochte websites of applicaties, en het datagebruik via het draadloze netwerk, wordt bijgehouden in logboeken en kan desgevallend wel geanalyseerd worden, als het globale verbruik dit rechtvaardigt. Alle informatie hier aangaande wordt strikt vertrouwelijk behandeld.

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).

3. BEVEILIGING EN CONTROLE OP INTERNETVERKEER

Op Vrij Katholiek Basisonderwijs De Wegwijzer 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 Vrij Katholiek Basisonderwijs De Wegwijzer verantwoordelijk voor het algehele dataverbruik, en voor alles dat er met / via deze internetverbinding gebeurt. Daarom hanteert men ook hier een aantal regels en controles daarop:

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

4. BEVEILIGING EN CONTROLE OP TOESTELLEN VAN DE SCHOOL

Onder “toestellen” van de school rekenen we zowel desktop computers, laptops, tablets als (eventuele) werk-smartphones die eigendom zijn van de school.

4.1. Algemeen

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

- Het internetverkeer en gebruikte toepassingen wordt, op verscheidene niveau’s, gecontroleerd inzake bv. bezochte doelsites, uitgaand verkeer, capaciteit maar ook veiligheid van de toepassing, het al dan niet veranderen van systeeminstellingen (gerelateerd aan beveiliging resp. prestaties, enz.).
- 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 Vrij Katholiek Basisonderwijs De Wegwijzer dan ook verschillende maatregelen genomen om dit te verhinderen. Het doelbewust veranderen van systeem- of beveiligingsinstellingen is verboden.

Dit beleid wordt gecombineerd met een aantal monitoring tools en/of (lokale) logboeken, d.w.z. manieren om de handelingen bij te houden voor analyse of eventueel naar bewijslast toe. De algemene maatregelen (zie § 1.2) worden toegepast, met i.h.b. logging van: tijdsregistratie, MAC- en IP-adressen, gebruikersnamen, toestelnamen, logintijd, gebruikte toepassingen, wijzigingen in systeeminstellingen.

- Het is, met bepaalde tools, toegestaan dat de beheerders, directie en eventueel andere personeelsleden die hiervoor bevoegd geacht worden, 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, pda’s, tablets, smartphones) die bepaalde personeelsleden gebruiken maar die eigendom zijn van Vrij Katholiek Basisonderwijs De Wegwijzer, 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.

Vrij Katholiek Basisonderwijs De Wegwijzer voorziet in ‘Intune-licenties’ waarmee bepaalde veiligheidsinstellingen kunnen ‘afgedwongen’ worden, bv. vergrendeling, wissen op afstand, etc.

5. BEVEILIGING EN CONTROLE OP TOESTELLEN VAN EINDGEBRUIKERS ZELF

Op Vrij Katholiek Basisonderwijs De Wegwijzer 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 Vrij Katholiek Basisonderwijs De Wegwijzer, 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 -beleid, zijn:

Het internetverkeer en gebruikte toepassingen wordt, op verscheidene niveau's, gecontroleerd inzake bv. bezochte doelsites, uitgaand verkeer, 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, logintijd, gebruikte toepassingen, wijzigingen in systeeminstellingen, enz.

Alle persoonlijke toestellen die binnen het netwerk van Vrij Katholiek Basisonderwijs De Wegwijzer gebracht worden dienen voorzien te zijn van een antivirusprogramma dat up-to-date is.

5.2. Vergrendeling, encryptie, antivirusbeveiliging en wissen van op afstand

De mobiele toestellen (d.w.z. laptops, pda's, tablets, smartphones) van medewerkers, waarop persoonsgegevens van Vrij Katholiek Basisonderwijs De Wegwijzer 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.
- Personeelsleden die op hun smartphone o.a. e-mails, Office 365, etc. van Vrij Katholiek Basisonderwijs De Wegwijzer willen raadplegen zijn verplicht dit toestel 'onder beheer' van Vrij Katholiek Basisonderwijs De Wegwijzer te stellen. Concreet betekent dit dat Katholiek een vergrendeling van het toestel kan afdwingen en/of het toestel vanop afstand wissen. Dit betekent geenszins dat Vrij Katholiek Basisonderwijs De Wegwijzer toegang heeft tot de inhoud van het toestel.

6. PRAKTISCHE AFSPRAKEN

6.1. Toestellen eigendom van de school

1. Alle toestellen (mobiel of niet mobiel) worden, in de mate van het mogelijke, steeds voorzien van de laatste beveiligingsupdates.
2. Toestellen met een besturingssysteem waarvoor Microsoft geen beveiligingsupdates meer uitbrengt (o.a. Windows XP, Windows Vista) worden buiten dienst of geüpgraded naar een ander besturingssysteem).
3. Alle toestellen worden voorzien van een up-to-date antivirussysteem.
4. Alle toestellen waarmee (door leerkrachten) persoonsgegevens kunnen geraadpleegd worden, worden voorzien van afzonderlijke accounts per leerkracht. Voor computers die enkel door leerlingen gebruikt worden hoeft dit niet noodzakelijk.
5. Computers die gebruikt worden om persoonsgegevens te raadplegen worden voorzien van een automatische vergrendeling (ingesteld op max. 30 min)
6. Het personeelslid zal de toestellen van de school behandelen als 'een goede huisvader'.
7. Het is niet toegestaan systeeminstellingen te wijzigen op toestellen van de school en/of software te kopiëren.
8. Nieuwe software mag enkel geïnstalleerd worden na voorafgaandelijke toestemming van de netwerkbeheerder en/of de ICT-coördinator. Leg de grootste omzichtigheid aan de dag bij het installeren van nieuwe software en klik niet zomaar blindelings op ok en volgende (zo vermijd je eventueel ongewenst spyware te installeren).
9. In geen geval zal het personeelslid toestellen en/of het netwerk van Vrij Katholiek Basisonderwijs De Wegwijzer gebruiken om onoorbare websites te bezoeken.
10. Van toestellen van Vrij Katholiek Basisonderwijs De Wegwijzer die definitief buiten dienst gesteld worden, dient de harde schijf fysiek vernietigd te worden.
11. Toestellen eigendom van Vrij Katholiek Basisonderwijs De Wegwijzer mogen niet meegenomen worden naar huis.
12. Toestellen eigendom van Vrij Katholiek Basisonderwijs De Wegwijzer mogen buiten de schoolmuren wel gebruikt worden voor uitzonderlijke schoolse activiteiten in opdracht van de directeur.

6.2. Toestellen eigendom van het personeelslid

1. Eigen toestellen van het personeelslid maken enkel verbinding met het BYOD-netwerk van de school (indien beschikbaar).
2. Het personeelslid draagt er zorg voor dat zijn antivirusprogramma up-to-date is.
3. In de mate van het mogelijke is de account van het personeelslid beveiligd met een wachtwoord.
4. Het personeelslid waakt erover dat gezinsleden of derden geen toegang krijgen tot de persoonsgegevens die Vrij Katholiek Basisonderwijs De Wegwijzer in bewaring heeft.

6.3. USB-STICKS

1. Vrij Katholiek Basisonderwijs De Wegwijzer ontmoedigt het gebruik van onbeveiligde USB-sticks.
2. **Onder geen enkel beding** worden persoonsgegevens (rapporten, klasprofielen, etc.) opgeslagen op een niet geëncrypteerde (=onbeveiligde) USB-stick. Gebruik van een beveiligde USB-stick is wel toegestaan.
3. Personeelsleden van Vrij Katholiek Basisonderwijs De Wegwijzer gebruiken voor de opslag van persoonsgegevens bij voorkeur het ter beschikking gestelde online opslagmedium OneDrive for Business dat onder beheer staat van de scholengemeenschap en dat een voldoende veilige toegang waarborgt.
4. Het gebruik van persoonlijke online opslagmedia (Google Drive, Dropbox, OneDrive Personal, …) is niet toegestaan voor het bewaren van persoonsgegevens in beheer van Vrij Katholiek Basisonderwijs De Wegwijzer.

6.4. Datalekken

- Onder datalekken verstaat Vrij Katholiek Basisonderwijs De Wegwijzer onder andere elk verlies/diefstal van een toestel (computer, laptop, tablet, smartphone, USB-stick,...) waarop persoonsgegevens staan of waarmee toegang kan verkregen worden tot deze persoonsgegevens.
- Elk datalek dient **onmiddellijk** gemeld te worden bij de aanspreekpunten informatieveiligheid (AIV's) via het e-mailadres privacy@ko-dewegwijzer.be