ACHTERGRONDINFORMATIE

Don Bosco Onderwijscentrum

voor:

Don Bosco De Puzzel Haacht

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

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	02/05/2018	GELDIG		

1 *Wachtwoordbeleid – Phishing: hengelen naar gegevens …*

1.1 Wat is phishing?

Je zal zelf weleens een e-mail hebben gekregen die leek te komen van de bank of het telecombedrijf waar je al dan niet klant bij bent. In de mail wordt meestal gevraagd om op een link te klikken en dan je persoonlijke gegevens zoals naam, pincode, bankgegevens, wachtwoord… in te vullen. Waarschijnlijk word je in de mail ook gevraagd om het snel te doen. De reden die de mail opgeeft zijn uiteenlopend maar klinken heel realistisch: bijvoorbeeld omdat je achterstaande betalingen hebt en je anders een boete krijgt, of omdat er verdachte activiteiten zijn opgemerkt omtrent het gebruik van je kredietkaart maar het kan ook gewoonweg gaan omdat we je gegevens willen controleren.
Het aanmanen om het snel te doen is wel heel cruciaal omdat jij dan gewoon minder snel nadenkt en sneller gaat 'bijten'.

Eens je echter op de link klikt, word je naar een valse website geleid die lijkt op het officiële portaal: een *gespoofte* website. Meestal een nagemaakte website met een adres dat enorm goed lijkt op de originele (voorbeeld zou zijn www.beltius.be i.p.v. www.belfius.be) Indien je daar je gegevens zou invullen, worden ze rechtstreeks naar een cybercrimineel gestuurd die uit is op jouw informatie. Het kan ook dat je via de link malware op je computer krijgt, zoals een keylogger die je informatie bijhoudt, of ransomware, die je bestanden of je volledige computer versleutelt.

Dat is een voorbeeld van phishing, maar het fenomeen beperkt zich allerminst tot die exacte situatie. Phishing is een vorm van social engineering waarbij een cybercrimineel gegevens of geld van een gebruiker probeert te stelen. En dat kan op heel veel verschillende manieren.

1.2 Soorten phishing

Phishing gebeurt meestal via e-mail, hoewel het ook via een app, valse website, of ook telefonisch kan. Hieronder de meest voorkomende soorten:

Spearphishing: Leunt erg aan bij standaardphishing, alleen gaat het hier niet om een willekeurig doelwit. *Een specifiek slachtoffer* wordt uitgekozen en het bericht wordt gepersonaliseerd om de persoon te doen geloven dat het om een legitieme boodschap gaat. Vaak doet men wat social engeneering om jouw te doen geloven dat de mail afkomstig is van je baas of van een bepaalde persoon uit je werkomgeving dienst die je vertrouwt.

Whaling: Spearphishing, maar dan gericht op de "grote vissen": managers, directeurs, CEO's, CFO's, en dergelijke. In plaats van één werknemer in de luren te leggen, mikt deze aanval op het groffe geld. De login-gegevens van de managers kunnen immers gebruikt worden om bedrijfskritische gegevens te stelen of phishing-mails naar honderden werknemers tegelijkertijd te sturen. Wie gaat er ooit een mail weigeren die effectief van de CEO komt?

Pharming: In plaats van te vissen, kiezen sommige cybercriminelen er ook voor om te oogsten. Met pharming worden nietsvermoedende gebruikers bij het surfen omgeleid worden. Dat kan bijvoorbeeld door een gehackte DNS-server. Zelfs wanneer de gebruiker dan de juiste url ingeeft, wordt hij nog omgeleid naar een valse website. Doelwitten zijn bijvoorbeeld de website van je bank, of van een sociaal netwerk. Wanneer je inlogt, zijn je gegevens niet langer privé.

1.3 Hoe herken je phishing?

Enkele jaren terug was het nog niet eens bijster moeilijk om een phishing-mail te herkennen, vooral niet in het Nederlands. De taal die werd gebruikt in de mail was vaak doorspekt met spelfouten en grammaticale flaters op een manier die zelfs de grootste taalbarbaar nauwelijks kon ontgaan. De huidige trend geeft echter aan dat cybercriminelen iets meer werk steken in de geloofwaardigheid van hun phishingmails. Veel van die mails zijn haast niet te onderscheiden van de *real deal*. Je kan wel een paar stappen overlopen om twijfel uit te sluiten.

Let op de begroeting: Rudimentaire phishing-mails die in bulk worden verzonden, beginnen vaak met een heel generische begroeting, zoals “Geachte klant” of “Beste collega”. Het is geen waterdicht signaal, aangezien spearphishing-mails wel gepersonaliseerd zijn, maar er moet een lampje gaan branden als het zo is.

Wat wordt er gevraagd: Een echte bank, telecombedrijf of andere instantie zal nooit via e-mail vragen om je gegevens te bevestigen, of andere informatie in te geven, via een link. Als het bovendien dringend moet, kan je ervanuit gaan dat ze zullen bellen.

Check de link: De link in phishing-mails beschrijft vaak de officiële pagina in de linktekst, maar leidt eigenlijk naar een heel andere website. Controleer de eindbestemming door over de link te zweven. Je kan de url dan linksonder in de hoek van je scherm bekijken.

Bij twijfel kan je altijd bellen naar de officiële instantie zelf. Doe dat dan aan de hand van een telefoonnummer dat je op een onafhankelijke website vindt, en dus niet het nummer dat eventueel in de mail te vinden is. Als je belt, kan de organisatie makkelijk zeggen of de mail legitiem is, of niet, en kunnen ze toekomstige klanten sneller waarschuwen voor frauduleuze e-mails.

2 *Communicatiebeleid – Nettiquette*

Bron: https://www.leren.nl/rubriek/computers_en_internet/internetten/nettiquette/

2.1 Wanneer wel e-mail, wanneer niet?

‘Uit onze administratie blijkt dat uw dienstverband bij de Rijksuniversiteit is beëindigd’. Dit bericht vonden de 7.000 medewerkers van de Rijksuniversiteit Groningen op een maandagochtend in november 2006 in hun mailbox. Gelukkig bleek het om 'fout’ in het computersysteem' te gaan. Waarom het automatisch gegenereerde mailtje naar duizenden medewerkers was gestuurd, was een groot raadsel. Nadat de fout was ontdekt, volgde meteen een excuusmail waarin de medewerkers werd verzekerd dat het een foutief bericht betrof en zij zich geen zorgen hoefden te maken over hun baan. De hele affaire had honderden bezorgde telefoontjes en e-mails tot gevolg.

Minder fortuinlijk waren de 400 medewerkers van een Amerikaanse elektronicaketen RadioShack in september 2006. Zij werden per e-mail op de hoogte gebracht van hun ontslag en konden meteen hun spullen pakken. ‘Omwille van de efficiency’, had de directie van het bedrijf voor deze werkwijze gekozen. De medewerkers waren woedend en vonden de werkwijze ‘onmenselijk en respectloos’.

E-mail is in lang niet elke situatie het juiste communicatiemiddel. Denk bijvoorbeeld aan zaken die iemand persoonlijk raken, zoals de beëindiging van een dienstverband. Dit hoort in een persoonlijk gesprek besproken te worden. Of als je een vraag hebt waar je meteen antwoord op wilt, kun je beter de telefoon pakken of even bij je collega langsgaan en het hem vragen. Toch wordt e-mail regelmatig gebruikt in situaties waarin een persoonlijk gesprek beter op zijn plaats was geweest. Niet zelden leidt dit - vaak ondoordacht – automatisme tot irritaties, woede en misverstanden. Vraag je bij elk bericht even af of het wel verstandig is voor de betreffende boodschap e-mail als medium te gebruiken.

Situaties waarin je e-mail kunt gebruiken

Je kunt e-mail gebruiken als je:

- Een afspraak wilt maken met 1 of meerdere personen
- Een afspraak wilt bevestigen
- Een eenvoudige vraagt hebt
- Een vraag hebt waar je niet snel een antwoord op hoeft te krijgen
- Een antwoord moet geven op een eenvoudige vraag
- Aan veel mensen tegelijk een mededeling wilt doen (en die niet heel belangrijk is)
- Een vergadering wilt plannen
- Iemand wilt bereiken die heel slecht bereikbaar is.

Situaties waarin je e-mail beter niet kunt gebruiken

Je kunt e-mail beter niet gebruiken als je:

- Een meningsverschil hebt
- Vertrouwelijke informatie wilt uitwisselen
- Slecht nieuws hebt
- In een situatie zit waar een probleem bestaat of dreigt te ontstaan
- Op het allerlaatste moment een vergadering of afspraak wilt afzeggen
- Veel vragen hebt
- Een vraag hebt waar je met spoed een antwoord op wilt hebben

- Vertrouwelijke informatie wilt uitwisselen
- Een vervelend bericht hebt.

Andere mogelijkheden

Wat kun je doen als e-mail niet het meest geschikte medium is?

- Loop bij je collega langs
- Pak de telefoon
- Maak een afspraak voor een persoonlijk gesprek
- Verstuur de informatie via de (interne) post
- Stuur een fax
- Spreek je collega aan in de kantine

2.2 Do's van e-mailen

Je typt een bericht, kiest een adres, drukt op verzenden en... klaar. Een kind kan de was doen. E-mail heeft haar populariteit te danken aan het gemak en de snelheid waarmee een berichtje kan worden verstuurd. Maar juist daardoor gaat het ook zo vaak mis: in de haast opgestelde berichten vol spelfouten, onduidelijke verzoeken en nutteloze mededelingen leiden tot irritatie, volle inboxen en veel tijdverlies, want al die e-mails moeten toch geopend en bekeken worden.

Wees helder en to the point

Verplaats je in de ontvanger van je e-mail en geef in de onderwerpregel bovenaan het bericht aan waar het over gaat. Je kunt bijvoorbeeld aangeven wat je van hem verlangt en - zonodig - wanneer. Ook kun je (duidelijk!) verwijzen naar eerdere e-mails. Bijvoorbeeld: '... in mijn mail van 24 september jl. met als onderwerp 'concept beleidsnota versie 1.2'. Het is dan voor de ontvanger meteen duidelijk of hij snel actie moet ondernemen of dat je bericht even kan wachten. Bovendien kan hij je bericht zo gemakkelijk terugvinden. Hiermee toon je niet alleen respect voor de tijd van een ander, je ontvangt waarschijnlijk ook een helder antwoord terug. Probeer je zoveel mogelijk tot één onderwerp te beperken. Heb je meerdere onderwerpen, spreid ze dan over meerdere e-mails. De ontvanger houdt zo het overzicht en kan je e-mails gemakkelijker afhandelen. Behandel je toch meer onderwerpen in je bericht, geef de onderwerpen dan een nummer.

Kom in de eerste alinea van je e-mailbericht meteen to-the-point. Wil je dat je collega de tweede versie van je concepttekst van commentaar voorziet, geef dat dan aan. Eventuele toelichting kun je daarna geven. Houd je bericht zo kort mogelijk, want het lezen van lange lappen tekst op een beeldscherm is niet prettig. Dreigt je e-mail toch erg lang te worden, voorzie je tekst dan van tussenkopjes.

Heb je dringend een reactie nodig, bel dan de ontvanger ook even om te zeggen dat je een e-mail hebt gestuurd. Je kunt zo de urgentie van je bericht nog eens benadrukken en de ontvanger kan aangeven of hij binnen de door jouw gestelde termijn kan reageren.

Overigens: gebruik voor de echte spoedgevallen niet de e-mail, maar pak de telefoon of loop even bij je collega langs.

Ga weloverwogen met bijlagen om

Met de bijlagenfunctie in je e-mailprogramma kun je bestanden met je e-mail meesturen. Hartstikke handig, alleen moet je ze wél daadwerkelijk toevoegen; het is weinig professioneel wanneer je in je e-mail naar een attachment verwijst dat ontbreekt. Je kunt dit voorkomen door er een gewoonte van te maken eerste de bijlage te selecteren en daarna pas het begeleidende bericht te schrijven. Schrijf altijd een begeleidende tekst bij een bijlage. Hierin leg je het doel van de bijlage uit en geef je precies aan wat je van de ontvanger verwacht.

Vraag je altijd af of het nodig is om de bijlage met je bericht mee te sturen. Staat de informatie al op het intranet of in een gedeelde map, dan is een link hiernaar voldoende. Zo voorkom je onnodig geheugengebruik in de mailbox van de ontvanger en overbelasting van het bedrijfsnetwerk. Bovendien hoeft de ontvanger minder handelingen te verrichten (bijlage openen, opslaan, verwijderen).

Wanneer je een bijlage meestuurt, let er dan op dat het bestand een duidelijke naam heeft en niet te groot is. Nietszeggende bestanden, zoals verslag.doc, en grote bestanden die niet snel geopend kunnen worden, wekken irritaties op bij de ontvanger. Nog erger is het wanneer je bijlage een virus blijkt te bevatten. Controleer bijlagen dan ook altijd op grootte en virussen.

Beperk het gebruik van cc

In sommige organisaties slibben inboxen helemaal dicht door de enorme hoeveelheid cc’tjes die worden verstuurd. Veelal heeft dit met de bedrijfscultuur te maken. Wees selectief in het versturen van zogenoemde cc'tjes. Gebruik cc alleen als het echt nodig is voor de ontvanger.

Let op correcte adressering

In de haast kan het wel eens gebeuren dat je een adres verkeerd intikt, de verkeerde contactpersoon in je adresboek selecteert of iemand vergeet. Controleer bij het verzenden van een bericht altijd of je het bericht aan de juiste perso(o)n(en) hebt geadresseerd. Vooral bij gevoelige informatie kan een dubbele check geen kwaad. Voorzie externe mail altijd van een disclaimer. In het geval een bericht bij de verkeerde persoon wordt bezorgd, zorgt deze ervoor dat derden hieraan geen rechten kunnen ontlenen of het bedrijf aansprakelijk kunnen stellen.

Let op formulering en spelling

Gaan we voor een brief nog eens goed zitten, bij het schrijven van een e-mail lijken goede omgangsvormen en spellingsregels te verdwijnen als sneeuw voor de zon: berichten vol spelfouten waarin alleen het hoognodige wordt vermeld. Hoewel zo niet bedoeld, kun je bij de ontvanger zo ongenuanceerd en kortaf overkomen.

Natuurlijk maakt het uit naar wie je de e-mail verstuurt - een snelle boodschap aan een collega kan informeler dan een bericht aan een klant - maar een correcte spelling en een goede formulering is ook een kwestie van fatsoen. Bovendien kom je met een goed geformuleerd en een juist gespelde tekst professioneler over dan met een rommelig bericht. Lees een e-mail dus goed door voor je hem verzendt en gebruik je spelling- en grammaticacontrole.

Wees ook voorzichtig met ironie, sarcasme en humor. Door het ontbreken van fysiek contact kan een grap gemakkelijk als kritiek worden uitgelegd.

2.3 Don’ts van e-mailen

Zet de ontvanger niet op het verkeerde been

Verstuur nooit een e-mail zonder het onderwerp in de onderwerpregel aan te geven. Verzend ook nooit een bericht zonder je naam te vermelden. Schrijf geen zinnen in hoofdletters. De ontvanger zal dit interpreteren als schreeuwen en zal denken dat je boos op hem bent.

Gebruik e-mail niet voor gevoelige onderwerpen of slecht nieuws

Hoewel e-mail in lastige situaties een aantrekkelijk alternatief lijkt, mag je je nooit achter een e-mail verschuilen. Door het ééndimensionale karakter van e-mail zie je niet hoe je bericht bij de ontvanger overkomt en kun je een misverstand niet meteen rechtzetten. Ook heb je geen idee van de omstandigheden en timing van het moment waarop je e-mail wordt gelezen. Hoe je slecht nieuws wel kunt brengen, leer je in de cursus Gesprekstechnieken.

Verzend geen vertrouwelijke informatie

In principe is e-mail niet geschikt voor het uitwisselen van vertrouwelijke informatie. Ook privé-informatie over collega’s wissel je niet uit via de mail. Een e-mail - of de reactie daarop – wordt nogal eens naar anderen doorgestuurd en dan komt je bericht terecht bij mensen voor wie jij hem niet had bestemd. Wees je ervan bewust dat in veel organisaties de systeembeheerder toegang heeft tot je e-mail.

Bcc

Wanneer je een bericht aan meerdere zakelijke contacten verstuurt, is het niet zo professioneel als de e-mailadressen van de geadresseerden voor iedereen zichtbaar zijn. Er zijn organisaties die maar al te gemakkelijk gebruikmaken van deze adressen om spam te versturen. Gebruik in een dergelijk geval bcc (blind carbon copy). De adressen die je hier invoert, zijn dan niet zichtbaar voor de anderen.

Wees niet te gemakzuchtig

Stuur niet voor ieder wissewasje een e-mail. Vraag je bij elk bericht even af of het wel verstandig is voor de betreffende boodschap e-mail als medium te gebruiken. Is een telefoontje of rechtstreeks contact met de collega, die een paar kamers verderop zit niet effectiever? En hoewel het een verleidelijk alternatief is om niet zelf de archiefkast in te hoeven duiken, is het niet verstandig om een e-mail te versturen waarin je om informatie vraagt die je zelf gemakkelijk kunt opzoeken. Het is niet collegiaal en zal voor de nodige irritaties kunnen zorgen.

Cc

Vele inboxen slibben dicht door de grote hoeveelheid cc’tjes die ‘voor de zekerheid’ en ‘ter info’ worden verstuurd. Doe hier niet aan mee en wees selectief in het versturen van cc’tjes.

To: alle afdelingen

In veel organisaties is het mogelijk om een bericht te versturen naar alle medewerkers of de medewerkers van een organisatieonderdeel, bijvoorbeeld de afdeling IT of Personeelszaken. Dat kan erg efficiënt zijn, bijvoorbeeld wanneer de directie een belangrijk bericht heeft.

Maar al te vaak wordt deze mogelijkheid uit gemakzucht gebruikt, omdat de verzender van de e-mail niet goed weet aan wie hij zijn bericht moet richten en voor het gemak de hele afdeling maar adresseert. Een bron van onnodige frustratie bij alle niet-terechte ontvangers.

Gebruik e-mail niet voor niet-zakelijke mail

Kettingbrieven horen niet thuis op het werk. Dat geldt ook voor e-mails die kwetsend kunnen zijn door grappen over huidskleur, afkomst, religie, seksuele geaardheid, ras of sekse. Gebruik je e-mail op het werk ook niet voor het verhandelen van spullen. De meeste organisaties hebben hier een speciaal hoekje voor ingericht op het intranet.

2.4 Checklist do's en don'ts

Do's	**Don'ts**
Let op formulering en spelling • Wees voorzichtig met ironie, sarcasme en humor • Voorkom spellingsfouten: lees je e-mail voor verzenden goed door en gebruik de spellingcontrole Wees helder en to the point • Zet in de onderwerpregel wat je van de ontvanger verwacht en wanneer • Begin je e-mail met je boodschap gevolgd door een toelichting • Behandel één onderwerp per e-mail • Behandel je meer onderwerpen per e-mail, nummer de onderwerpen dan • Houd je e-mail kort en zakelijk • Vraagt je e-mail echt snelle actie, bel dan de geadresseerde ook even op Ga weloverwogen met bijlagen om • Schrijf altijd een begeleidende tekst bij een bijlage: leg hierin uit wat het doel van de bijlage is en wat je van de ontvanger verwacht. • Vergeet de bijlage niet mee te sturen: leer jezelf aan eerst de bijlag te selecteren, daarna stel je de begeleidende mail op • Vraag je af of het noodzakelijk is om de bijlage toe te voegen of een alleen een link voldoende is • Voorzie de bijlage van een duidelijke naam • Controleer bijlagen altijd op grootte en virussen Beperk het gebruik van cc • Gebruik cc alleen als het echt nodig is voor de ontvanger. Let op correcte adressering • Controleer altijd of je je e-mail aan de juiste perso(o)n(en) adresseert • Voorzie externe e-mails altijd van een disclaimer	Zet de ontvanger niet op het verkeerde been • Verstuur nooit een e-mail zonder het onderwerp in de onderwerpregel aan te geven • Verzend ook nooit een e-mail zonder je naam te vermelden • Schrijf geen zinnen in hoofdletters • Verschuil je nooit achter een e-mail Verzend geen vertrouwelijke informatie • Verzend geen vertrouwelijke informatie of privé-informatie over collega's • Stuur e-mailadressen niet open en bloot mee als je een bericht verstuurt naar meerdere externe contacten Wees niet te gemakzuchtig • Stuur niet voor ieder wissewasje een e-mail • Vraag niet om informatie die je zelf gemakkelijk had kunnen opzoeken • Verstuur niet aan een hele afdeling een e-mail als je niet precies weet aan wie je je bericht moet richten • Ben niet gemakkelijk in het versturen van cc'tjes Gebruik e-mail niet voor niet-zakelijke mail • Doe niet mee aan kettingbrieven of ander 'grappen' • Gebruik je e-mail niet voor het verhandelen van spullen

INFORMATIEVEILIGHEIDS- EN PRIVACYBELEID

Don Bosco Onderwijscentrum

voor:

Don Bosco De Puzzel Haacht

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	02/05/2018	GELDIG		

Inhoud

1 Inleiding

Informatie en ict zijn noodzakelijk in de ondersteuning van het onderwijs. Denken we maar aan de leerlingadministratie- en leerlingvolgsystemen, agenda- en rapportprogramma's, oefen- en toetssystemen…. Vaak verwerken deze geautomatiseerde systemen persoonsgegevens (van leerlingen, ouders, lesgevers…) en is de privacywetgeving (AVG) hierop van toepassing.

Deze informatieverwerking en het gebruik van ict brengen risico's met zich mee. Denken we bijvoorbeeld maar aan een cyberaanval waarbij de gegevens versleuteld worden, een vergissing waardoor gegevens onherroepelijk gewist zijn, de natuur (bijv. overstroming of brand), et cetera. Het niet beschikbaar zijn van ict, incorrecte administraties en het uitlekken van gegevens kan leiden tot inbreuken op het geven van onderwijs en het vertrouwen in onze school.

Deze bedreigingen maken het noodzakelijk om adequate maatregelen te nemen op het gebied van informatieveiligheid en privacy (IVP) om de risico's die gepaard gaan met deze bedreigingen tot een aanvaardbaar niveau te reduceren. Om dit structureel op te pakken is het noodzakelijk dat we een duidelijk maken waar het om gaat, een doel stellen en de manier waarop we dit doel willen bereiken.

1.1 Toelichting informatieveiligheid

Onder informatieveiligheid wordt verstaan: het nemen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatie en ict zo maximaal mogelijk te garanderen.

Deze kwaliteitsaspecten zijn:

- **Beschikbaarheid:** de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- **Integriteit:** de mate waarin gegevens en/of functionaliteiten juist, volledig en actueel zijn.
- **Vertrouwelijkheid:** de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.
- **Controleerbaarheid:** de mate waarin het mogelijk is om achteraf parameters die van belang zijn voor beschikbaarheid, integriteit of vertrouwelijkheid te verifiëren.

Onvoldoende informatieveiligheid kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en bij de dagdagelijkse werking van de onderwijsinstelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imagoverlies.

1.2 Toelichting privacy

Privacy gaat over de verwerking van persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform de huidige wet- en regelgeving. De bescherming van de privacy regelt onder andere de voorwaarden waaronder persoonsgegevens gebruikt mogen worden.

Persoonsgegevens zijn hierbij alle gegevens van een geïdentificeerd of identificeerbaar individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. Denken we maar aan het verzamelen, raadplegen, bijwerken, verspreiden tot met het wissen van deze gegevens.

1.3 Vervlechting informatieveiligheid en privacy

Informatieveiligheid is noodzakelijk om privacy te waarborgen. Beide begrippen zijn met elkaar verbonden. Het onderwerp informatieveiligheid en privacy wordt afgekort tot IVP. Deze beleidstekst ligt ten grondslag aan de aanpak van informatieveiligheid en privacy binnen Don Bosco De Puzzel Haacht.

2 Doel en reikwijdte

2.1 Doel

Dit beleid heeft als doelen:

- Het waarborgen van de continuïteit van het onderwijs en de dagdagelijkse werking van Don Bosco De Puzzel Haacht.

- Het garanderen van de privacy van leerlingen en medewerkers waardoor beveiligings- en privacy-incidenten zoveel mogelijk worden voorkomen.

Dit beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een goede balans moet zijn tussen privacy, functionaliteit, veiligheid en middelen. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene, met name van medewerkers, leerlingen en ouders wordt gerespecteerd en dat Don Bosco De Puzzel Haacht voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Don Bosco De Puzzel Haacht waaronder in ieder geval: alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties, evenals op andere betrokkenen waarvan Don Bosco De Puzzel Haacht persoonsgegevens verwerkt.

- Dit beleid is van toepassing op zowel de digitale als geschreven verwerking van persoonsgegevens.

- Het IVP-beleid geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties die uit hoofde van hun taak, op school of thuis persoonsgegevens verwerken.

- Het beleid heeft betrekking op gecontroleerde informatie die door onszelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en sociale media. Hiervoor werkt Don Bosco De Puzzel Haacht met **gedragscodes**.

- Het IVP-beleid binnen Don Bosco De Puzzel Haacht heeft raakvlakken met:
  - Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulp-verlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen;
  - Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties;
  - IT-beleid; met als aandachtspunten de aanschaf, het beheer, het gebruik en/of het uit dienst stellen van hardware, software, services en (digitale) leermiddelen;
  - Participatie van leerlingen, hun ouders/verzorgers en medewerkers.

3 Uitgangspunten

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij Don Bosco De Puzzel Haacht zijn:

- IVP dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de **Algemene Verordening Gegevensbescherming** (AVG).
  De verwerking van persoonsgegevens is steeds gebaseerd op één van de in deze verordening vastgelegde rechtmatigheden. Hierbij willen we een goede balans zoeken tussen het belang van Don Bosco De Puzzel Haacht om persoonsgegevens te verwerken en het belang van de betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn/haar persoonsgegevens.

- Het schoolbestuur, Don Bosco Onderwijscentrum, is als rechtspersoon de **verwerkingsverantwoordelijke** voor alle persoonsgegevens die in opdracht van Don Bosco De Puzzel Haacht verwerkt worden.

- Don Bosco De Puzzel Haacht beheert ook informatie waarvan de intellectuele eigendom (het **auteursrecht**) toebehoort aan derden. Medewerkers en leerlingen moeten dus goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.

- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt daarom bij Don Bosco De Puzzel Haacht geclassificeerd. Deze **classificatie** vormt het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risico-analyse, waarbij gebruik gemaakt wordt van de classificatie. Het beleid maakt een balans tussen de risico's van hetgeen we willen beschermen en de benodigde maatregelen.

- Don Bosco De Puzzel Haacht sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) **verwerkersovereenkomsten** af indien deze persoonsgegevens ontvangen van de school.

- Binnen Don Bosco De Puzzel Haacht is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van **iedereen**. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van fysieke documenten.

- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. In het *algemeen reglement van het personeel van het katholiek onderwijs* (artikel 7 § 7) wordt hiernaar verwezen.

- Bij wijzigingen in de infrastructuur, de aanschaf en de uit dienst name van (informatie)systemen, wordt bij Don Bosco De Puzzel Haacht steeds rekening gehouden met IVP.

- IVP is bij Don Bosco De Puzzel Haacht een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

3.2 Uitgangspunten privacy

De zes vuistregels met betrekking tot de omgang van persoonsgegevens bij Don Bosco De Puzzel Haacht zijn:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op één van de wettelijke rechtmatigheden: toestemming, overeenkomst, wettelijke verplichting, openbaar belang, vitaal belang van de betrokkene of gerechtvaardigd belang.
3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken. Ze staan in verhouding tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt.
4. **Transparantie**: de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IVP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op inzage, verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Opslagbeperking:** data wordt niet langer bewaard dan noodzakelijk. De verwerking wordt door het IVP-beleid beperkt in de tijd.
6. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn, en dat zij voldoende beschikbaar zijn om de werking van Don Bosco De Puzzel Haacht te waarborgen. Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van **toestemming**, zal Don Bosco De Puzzel Haacht een eenduidige procedure hanteren die een actieve en aantoonbare handeling vereist.

4 Wet- en regelgeving

Don Bosco De Puzzel Haacht voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Algemene Verordening Gegevensbescherming (AVG)
- Camerawet
- Auteurswet

5 Organisatie

De organisatie van IVP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Dit hoofdstuk beschrijft hoe IVP in Don Bosco De Puzzel Haacht is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Voor elk niveau wordt beschreven welke verantwoordelijkheden en taken de verschillende rollen met zich meebrengen.

5.1 Rollen (functies) rondom IVP

Om IVP gestructureerd en gecoördineerd aan te pakken worden bij Don Bosco De Puzzel Haacht een aantal rollen aan medewerkers in de bestaande organisatie toegewezen.

5.2 Richtinggevend

Verwerkingsverantwoordelijke

Het schoolbestuur is eindverantwoordelijk voor IVP en stelt het beleid en de basismaatregelen op het gebied van IVP vast.

De toepassing en werking van het IVP-beleid wordt op basis van regelmatige rapportages geëvalueerd.

Zie bijlage 1 voor een schematische weergave van de rol- en taakverdelingen aangaande IVP op Don Bosco De Puzzel Haacht en binnen Don Bosco Onderwijscentrum.

5.3 Sturend

Data Protection Officer (DPO) van de koepelorganisatie

Vanuit de koepelorganisatie Katholiek Onderwijs Vlaanderen wordt er een Data Protection Officer aangesteld. Deze zal binnen het schoolbestuur of instelling het Aanspreekpunt Informatieveiligheid (AIV) aansturen. De taak bestaat uit:

- schoolbesturen informeren en adviseren over hun verplichtingen vanuit de AVG en vanuit andere gegevensbeschermingsbepalingen;
- AIV's opleiden en hulpmiddelen verstrekken zodanig dat ze binnen hun instelling(en) het IVP-beleid kunnen ondersteunen;
- desgevraagd advies verstrekken over de gegevensbeschermingseffectbeoordeling;
- met de toezichthoudende autoriteit samenwerken en optreden als aanspreekpunt voor deze autoriteit.

Aanspreekpunt Informatieveiligheid

Het AIV is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (directie van de instelling, raad van bestuur van het schoolbestuur) en staat de mensen op uitvoerend niveau bij. Het AIV moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen Don Bosco De Puzzel Haacht
- Meewerken aan de bewustmaking en opleiding van het personeel
- Het aanspreekpunt zijn voor incidenten op het gebied van IVP
- De verdere afhandeling van incidenten binnen Don Bosco De Puzzel Haacht coördineren

Domeinverantwoordelijke / proceseigenaar

Binnen elke instelling zijn er verschillende domeinen/processen, zoals bv. ict, personeel, administratie, facilitaire en financiële zaken, onderwijs et cetera. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IVP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

De proceseigenaar is verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben proceseigenaren de volgende specifieke taken:

- *Samen met de raad van bestuur / de directie stellen zij het beleid voor toegang vast.*
- *Samen met het functioneel beheer en ict zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.*
- *Samen met het functioneel beheer en ict beoordelen zij regelmatig de toegangsrechten van gebruikers.*

Leidinggevenden hebben een voorbeeldrol ten opzichte van hun medewerkers.

5.4 Uitvoerend

Leidinggevende

Naleving van het Informatieveiligheidsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid;
- toe te zien op de naleving van het IVP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IVP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IVP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door het AIV.

Ict-coördinator

De ict-coördinator vormt een technisch aanspreekpunt inzake informatieveiligheid voor het management en de medewerkers, en zorgt in de praktijk voor de implementatie van toegangsrechten en de rapportage aangaande digitale informatieveiligheid.

Functioneel beheerder

De functioneel beheerder wordt vanuit de domeinverantwoordelijke / proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

Medewerker

Alle medewerkers hebben een verantwoordelijkheid met betrekking tot informatieveiligheid in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het privacyreglement en eraan toegevoegde nota's en visieteksten aangaande IVP op Don Bosco De Puzzel Haacht. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists, formulieren en praktische tools.

Medewerkers wordt gevraagd om actief betrokken te zijn bij informatieveiligheid. Dit kan door meldingen te maken van veiligheidsincidenten, het doen van voorstellen ter verbetering van IVP en het uitoefenen van invloed op het beleid (individueel of via de ervoor voorziene overlegorganen en/of via het aanspreekpunt). Zelf hebben zij ook een voorbeeldfunctie naar andere medewerkers, externen en vooral leerlingen toe.

Van ambtswege uit, of eventueel contractueel, worden alle medewerkers (ook extern) van Don Bosco De Puzzel Haacht die toegang kunnen hebben tot persoonsgegevens, gebonden aan een discretieplicht. Welbepaalde (externe) medewerkers zijn wettelijk gebonden aan een beroepsgeheim.

6 Controle en rapportage

Dit IVP-beleid en alle bijhorende richtlijnen, nota's en tools, worden minimaal elke twee jaar getoetst en bijgesteld door het schoolbestuur. Hierbij wordt rekening gehouden met:

- De status van de informatieveiligheid als geheel (beleid, organisatie, risico's)
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent Don Bosco De Puzzel Haacht een jaarlijks planning en controlecyclus voor IVP. Dit is een vast evaluatieproces waarmee de inhoud en effectiviteit van het IVP-beleid wordt getoetst.

Voor alle overlegmomenten geldt dat deze zoveel mogelijk ingepast worden in bestaande overlegvormen met hetzelfde karakter waarbij op:

- **strategisch** niveau (richtinggevend) wordt gesproken over organisatie, alsmede over doelen, bereik en ambitie op het gebied van IVP.
- **tactisch** niveau (sturend) de strategie wordt vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.
- **operationeel** niveau (uitvoerend) de onderwerpen worden besproken die de dagelijkse uitvoering aangaan. Deze overlegvorm wordt niet centraal georganiseerd, en indien nodig in elk organisatieonderdeel van Don Bosco De Puzzel Haacht afzonderlijk.

6.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatieveiligheid en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij Don Bosco De Puzzel Haacht het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn onder andere de regelmatig terugkerende bewustwordingscampagnes voor iedereen binnen de school. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van het AIV en leidinggevende(n), met de raad van bestuur van Don Bosco Onderwijscentrum als eindverantwoordelijke.

6.2 Classificatie en risicoanalyse

Bij Don Bosco De Puzzel Haacht heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. De risicoanalyse zal het niveau van de beveiligingsmaatregelen bepalen rekening houdend met de classificatie van de gegevens. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang zijn voor de informatievoorziening.

6.3 Incidenten en datalekken

Bij Don Bosco De Puzzel Haacht is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

Alle incidenten kunnen worden gemeld bij privacy@depuzzelhaacht.be. De afhandeling van deze incidenten volgt een gestructureerd proces, waarbij men ook voorziet in de juiste stappen rondom de meldplicht datalekken.

6.4 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IVP proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij Don Bosco De Puzzel Haacht wordt actief aandacht besteed aan IVP bij de aanstelling, tijdens functioneringsgesprekken, met een gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Mocht de naleving ernstig tekort schieten, dan kan Don Bosco De Puzzel Haacht de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden. Voor de bevordering van de naleving van de AVG heeft het AIV een belangrijke rol.

Bijlage 1: Tabel IVP rollen en taken

Wie **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
School- of centrumbestuur	• Eindverantwoordelijke • IVP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IVP-beleid op basis van rapportages en bijsturen van dit beleid indien nodig • Organisatie IVP inrichten	• Informatieveiligheids- en privacy beleid opstellen en goedkeuren en communiceren • Aanspreekpunt informatieveiligheid aanstellen • Oprichten veiligheidscel
Leidinggevende (directie)	• Toezien op de naleving van het IVP-beleid en privacywetgeving en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Communicatie naar alle betrokkenen; er voor zorgen dat alle medewerkers op de hoogte zijn van het IVP-beleid en de consequenties ervan. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IVP-beleid. • Rapporteren voortgang m.b.t. doelstellingen IVP-beleid aan bestuur • Periodiek het onderwerp informatiebeveiliging onder de aandacht brengen in werkoverleg, beoordelingen,… • Implementeren IVP-maatregelen.	Communiceren, informeren en toezien op naleving van o.a.: • IVP in het algemeen • Hoe omgaan met leerlingendossiers • Wie mag wat zien • Gedragscode • Beveiliging van ruimtes • Preventieve maatregelen (o.a. brand en waterschade aan servers…) • …
Data protection officer koepel	• Schoolbesturen informeren en adviseren over hun verplichtingen krachtens de AVG en regelgeving; • Richtlijnen, kaders, procedures opstellen en aanbevelingen doen m.b.t. informatieveiligheid en privacy • Aanspreekpunten IVP opleiden en hen de nodige tools en hulpmiddelen verstrekken • desgevraagd advies verstrekken over de gegevensbeschermingseffectbeoordeling • samenwerken met de toezichthoudende autoriteit en optreden als aanspreekpunt voor deze autoriteit • Brugfiguur naar de externe partijen toe • Lerend netwerk ontwikkelen en aansturen	• Opstellen van algemene processen, richtlijnen en sjablonen IVP • Nascholingstraject organiseren • Overleg met informatieveiligheidsconsulenten onderwijsnetten en GO! • Overleg met externe partijen: leveranciers van leerlingadministratie en -volgsysytemen en leveranciers van didactische software • Tools aanpassen/ontwikkelen

Wie **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
Aanspreekpunt informatieveiligheid	• Informeert en adviseert directie/bestuur en personeel over IVP • Rapporteert naar directie/bestuur • Informeert de data protection officer van de koepel • Meewerken aan de uitwerking van een specifiek IVP-beleid op basis van het algemeen IVP-beleid • Voorstellen doen tot aanpassingen van centraal aangeboden processen, richtlijnen en procedures om de uitvoering van het IVP-beleid te ondersteunen binnen de school • Meewerken aan: o classificatie van middelen o risicoanalyse o het opstellen van een veiligheidsplan • Aanspreekpunt voor IVP-incidenten • Incidentafhandeling (registreren en evalueren). • Invullen register verwerkingsactiviteiten	Voorstellen van aanpassingen aan de uitgewerkte formulieren van processen, richtlijnen en procedures rond IVP, bijvoorbeeld: • Security awareness activiteiten • Authenticatie en autorisatie-beleid • Gedragscodes (ICT en internetgebruik, sociale media, privacybeleid…) naar medewerkers en leerlingen toe • Verwerkersovereenkomsten regelen • Toestemming opstellen gebruik foto's en video • Communicatieplan naar medewerkers, leerlingen, ouders en cursisten • Procedure IVP-incident afhandeling • Inrichten meldpunt datalekken • Melden datalekken naar de overheid toe • … Invullen van register verwerkingsactiviteiten voor schooleigen situatie
Informatieveiligheids cel (CIV) van de school of het schoolbestuur [1]	• Classificatie van informatie • IVP risicoanalyse uitvoeren • Prioriteiten voorstellen • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten bekrachtigen door bestuur • De toegangsrechten van gebruikers regelmatig beoordelen en controleren. • Evalueren IVP-beleid en voorstellen van verbetermaatregelen • Bespreking veiligheidsincidenten en voorstellen formuleren voor te nemen maatregelen • Aanpassen gegevensbeschermings-effectbeoordeling aan eigen situatie	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) • Classificatie van informatiebronnen en persoonsgegevens • Risicoanalyse uitvoeren en documenteren Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk
Iedereen	• Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IVP bij de dagelijkse werkzaamheden	Richtlijnen en procedures volgen Melden incidenten aan aanspreekpunt informatieveiligheid

[1] bestaande uit domeinverantwoordelijke/ proceseigenaren waaronder: ICT, personeelsdienst, preventieadviseur, financiën, leerlingenadministratie, facilitair management, leidinggevende en het aanspreekpunt informatieveiligheid

Bijlage 2: Aanvullende nota's

Bij dit algemene deel van het IVP-beleid horen nog enkele specifieke nota's :

- Classificatie van persoonsgegevens
- Toegangsmatrices
- Wachtwoordbeleid
- Communicatiebeleid
- Toestelbeleid
- Backupbeleid

Tevens is er een bijkomend document voorzien, dat de nodige achtergrondinformatie bij deze nota's.

BACKUPBELEID

Don Bosco Onderwijscentrum

voor:

Don Bosco De Puzzel Haacht

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

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	02/05/2018	GELDIG		

1 Inleiding

1.1 Situering

Voor de gegevens die een bepaald niveau van beschikbaarheid en/of integriteit vereisen, is een goed uitgestippeld back-upbeleid noodzakelijk. Deze principes gelden zowel voor gegevens die zich op NAS-en, servers, clients, eigen toestellen, andere locaties, in de cloud, … bevinden – zie ook het ***toestelbeleid*** en het BYOD-beleid in § 5 in het bijzonder.

Zie de ***classificatie van gegevens*** voor meer info aangaande de gehanteerde BIV-niveau's.

Deze nota valt onder de eindverantwoordelijkheid van Don Bosco Onderwijscentrum.

1.2 Enkele begrippen

UPS (*uninterrupted power supply*) Noodstroomvoorziening	*Aangesloten systemen en opslagmedia worden gedurende enkele minuten van stroom voorzien bij pannes of spanningsfluctuaties. Dit zorgt ervoor dat gegevens in het werkgeheugen en/of cache nog kan weggeschreven worden voordat het system afgesloten moet worden.*
Redundantie	*Het algemene principe waarbij een systeem, opslag of netwerkverbinding zo opgebouwd wordt, dat indien nodig een ander systeem overneemt. In principe mogen eindgebruikers hier niets van merken. Het "eerste" systeem dient zo snel mogelijk terug hersteld te worden.*
Back-ups	*Het nemen van geregelde kopieën, op een andere locatie en medium, zodat bij eventueel verlies of diefstal de gegevens in kwestie hersteld kunnen worden. De aard, frequentie, enz. van de backups wordt bepaald door de classificatie van de gegevens in kwestie. Dit proces kan volledig geautomatiseerd gebeuren.*
Synchronisatie	*Gegevens bevinden zich op verschillende locaties en media, maar een onderlinge netwerkverbinding zorgt ervoor dat beide kopieën hetzelfde zijn. Aanpassingen gebeuren m.a.w. steeds in beide kopieën tegelijk. Het systeem zorgt ervoor dat aanpassingen bijgehouden worden in het geval dat de verbinding (even) weg valt, om deze bij het herstellen van de verbinding zo snel mogelijk samen te voegen.*

2 Stroomvoorziening

Alle systemen waarop gegevens gebruikt of bewaard worden die behoren tot het beschikbaarheidsniveau ***noodzakelijk*** en/of het integriteitsniveau ***absoluut***, kunnen in Don Bosco De Puzzel Haacht voorzien worden van een redundante noodstroomvoorziening.

Gegevens die behoren tot het beschikbaarheidsniveau ***belangrijk*** en/of het integriteitsniveau ***vereist***, kunnen voorzien worden van een gewone sroomvoorziening.

3 Back-ups

Gegevens die behoren tot het beschikbaarheidsniveau ***belangrijk*** en/of het integriteitsniveau ***vereist***, kunnen geback-upt worden.

Alle andere gegevens kunnen minder frequent geback-upt worden.

Alle back-ups worden conform de gangbare “best practices” bewaard en (persoons)gegevens die behoren tot het vertrouwelijkheidsniveau ***vertrouwelijk*** of ***geheim***, kunnen geëncrypteerd geback-upt worden.

4 Brandveiligheid

De plaatsen op Don Bosco De Puzzel Haacht waar gegevens bewaard worden die behoren tot het beschikbaarheidsniveau ***belangrijk*** en/of het integriteitsniveau ***vereist***, of hoger, kunnen voorzien worden van afdoende brandbeveiligingsmaatregelen.

Indien deze gegevens (ook) bewaard worden op een andere locatie en/of bij (een) externe verwerker(s), dan legt Don Bosco Onderwijscentrum hieraan gelijkaardige eisen op.

CLASSIFICATIE VAN PERSOONSGEGEVENS

Don Bosco Onderwijscentrum

voor:

Don Bosco De Puzzel Haacht

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

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	03/02/2018	GELDIG		

1 Inleiding

1.1 Situering

Door een classificatie van persoonsgegevens te maken, kan men op Don Bosco De Puzzel op een gestructureerde manier de beveiliging van deze gegevens vorm geven. De classificatie gebeurt op basis van drie aspecten:

- beschikbaarheid;
- integriteit;
- vertrouwelijkheid.

Men spreekt ook wel eens van een BIV-classificatie. Voor elk aspect wordt in dit beleid een classificatie in niveau's gehanteerd, bv. **laag – midden – hoog**.

Op basis van de in deze nota uitgewerkte classificatie, bepaalt men op Don Bosco De Puzzel de nodige organisatorische en technische maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid gepast te waarborgen.

Deze nota valt onder de eindverantwoordelijkheid van Don Bosco Onderwijscentrum.

1.2 Hoe wordt het classificatieniveau bepaald?

Dit doen we op Don Bosco De Puzzel door gebruik te maken van de vragen, zoals deze zijn opgesteld voor het respectievelijke schema (zie onderstaande). Het is hierbij in zekere zin belangrijker om met een aantal mensen te praten over deze vragen, dan een exacte inschatting te maken. Door erover te praten kweek je bewustwording en ga je anders naar de processen kijken.

1.3 Welke persoonsgegevens worden er verwerkt?

Samengevat verwerkt Don Bosco De Puzzel de onderstaande categorieën van persoonsgegevens.

1.3.1 Leerlingen

- Rijksregister: *rijksregisternummer*
- Identificatie: *voornaam, naam, geboortedatum, geboorteplaats en/of identiteitskaartnummer*
- Pasfoto: *zoals op identiteitskaart, zelf genomen of via schoolfotograaf*
- Contact (school): *vast telefoonnummer, e-mailadres v.d. school, gsm-nummer v.d. school*
- Contact (privé): *eigen vast telefoonnummer, eigen e-mailadres, eigen gsm-nummer*
- Schoolloopbaan: *instellingen, jaren, richtingen, klassen*
- Afwezigheden: *afwezige (halve) dagen, redenen, bewijzen*
- Evaluatie: *puntenboeken, remediëring, rapporten, commentaren, deliberaties, verslagen, eindbeslissingen, motiveringen*
- Functioneren: *gedrag, welbevinden, communicatie met leerkrachten, medeleerlingen, groepsdynamiek, begeleiding, opvolging, straffen, sancties, tucht*
- Medische informatie: *zoals beschreven in wetgeving, ook zorgdiagnoses, -dossiers en medische begeleiding (intern en extern)*

1.3.2 Ouder(s) / voogd

- Identificatie: *voornaam, naam, geboortedatum, geboorteplaats en/of identiteitskaartnummer*
- Adres: *Straat, nummer, busnummer, postcode, gemeente, deelgemeente, land*
- Contact (privé): *eigen vast telefoonnummer, eigen e-mailadres, eigen gsm-nummer*
- Financieel: *bankgegevens, betaalde rekeningen, openstaande rekeningen, afbetalingen*

1.3.3 Personeel

- Rijksregister: *rijksregisternummer*
- Identificatie: *voornaam, naam, geboortedatum, geboorteplaats en/of identiteitskaartnummer*
- Pasfoto: *zoals op identiteitskaart, zelf genomen of via schoolfotograaf*
- Contact (school): *vast telefoonnummer, e-mailadres v.d. school, gsm-nummer v.d. school*
- Contact (privé): *eigen vast telefoonnummer, eigen e-mailadres, eigen gsm-nummer*
- Loopbaan: *sollicitatie, cv, diploma's, bekwaamheidsbewijzen, opdrachten, anciënniteit*
- Afwezigheden: *afwezige dagen, redenen, bewijzen*
- Evaluatie: *functioneringsgesprekken, evaluatiegesprekken*
- Levensbeschouwing: *indien (gedeeltelijk) leerkracht Godsdienst*

1.3.4 Oud-leerlingen

- Rijksregister: *rijksregisternummer*
- Identificatie: *voornaam, naam, geboortedatum, geboorteplaats en/of identiteitskaartnummer*
- Contact (privé): *eigen vast telefoonnummer, eigen e-mailadres, eigen gsm-nummer*
- Schoolloopbaan: *instellingen, jaren, richtingen, klassen*
- Evaluatie: *deliberaties, verslagen, eindbeslissingen, motiveringen*

1.3.5 Oud-personeel

- Rijksregister: *rijksregisternummer*
- Identificatie: *voornaam, naam, geboortedatum, geboorteplaats en/of identiteitskaartnummer*
- Contact (privé): *eigen vast telefoonnummer, eigen e-mailadres, eigen gsm-nummer*
- Loopbaan: *sollicitatie, cv, diploma's, bekwaamheidsbewijzen, opdrachten, anciënniteit*
- Evaluatie: *functioneringsgesprekken, evaluatiegesprekken*

2 Beschikbaarheid

2.1 Omschrijving

Hiermee bedoelen we de mate waarin de gegevens en diensten beschikbaar zijn, zodanig dat het onderwijsgebeuren ongestoord voort kan gaan.

Deelaspecten hiervan zijn:

- **Continuïteit:** de mate waarin de beschikbaarheid gewaarborgd is;
- **Portabiliteit:** de mate waarin de overdraagbaarheid van informatie naar andere gelijksoortige technische infrastructuren gewaarborgd is;
- **Herstelbaarheid:** de mate waarin de informatie of dienst tijdig en volledig hersteld kan worden in geval van onderbrekingen, pannes, onderhoud, ...

Voor de beschikbaarheid komt de classificatie respectievelijk overeen met: ***niet nodig, onbelangrijk, belangrijk, essentieel***.

Niveau 1: Beschikbaarheid is niet nodig	**Niveau 2:** Beschikbaarheid is onbelangrijk	**Niveau 3:** Beschikbaarheid is belangrijk	**Niveau 4:** Beschikbaarheid is noodzakelijk
Het systeem of de informatie is niet (meer) nodig voor de werking van de instelling.	*Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende meerdere dagen brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.*	*Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een dag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.*	*Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een werkdag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.*
Tussen 0 en 2	Tussen 3 en 7	Tussen 8 en 12	Tussen 13 en 15

2.2 Beschikbaarheidsschema

Dit schema moet per toepassing ingevuld worden.

Plaats een 'x' in de bijhorende kolom om de classificatie te maken, en motiveer elke vraag. Tel het eindtotaal op om de classificatie van de toepassing te bekomen (zie tabel in § 2.1). *0 staat voor "niet van toepassing"*.

Vragen	**0**	**1**	**2**	**3**	**Motivatie**
Wat is de verwachte belasting van de toepassing? *1 = weinig gelijktijdige gebruikers, weinig transacties* *2 = veel gelijktijdige gebruikers, normale hoeveelheid transacties* *3 = veel gelijktijdige gebruikers, veel transacties*					
Zijn er contractuele of wettelijke verplichtingen voor de beschikbaarheid? *1 = nee, of regulier* *2 = ruime of hoge contractuele verplichtingen* *3 = wettelijke verplichtingen, desgevallend enkel voor bepaalde periodes in het schooljaar*					
Wat is de maximale periode dat de toepassing niet- beschikbaar mag zijn (in de loop van het schooljaar)? *1 = maximaal enkele dagen of een week* *2 = maximaal een werkdag* *3 = maximaal een aantal uur*					
Hoe erg is het als de gegevens en/of de toepassing niet beschikbaar zijn? *1 = niet cruciaal voor de kerntaken* *2 = het lesgeven ondervindt hinder, maar kan doorgaan* *3 = het lesgeven (of cruciale deelaspecten ervan) kunnen niet doorgaan*					
Leidt het niet beschikbaar zijn van de toepassing tot imagoverlies? *1 = nee* *2 = kortstondig maar kan opgevangen of hersteld worden met goede communicatie* *3 = langdurig of blijvend imagoverlies*					

3 Integriteit

3.1 Omschrijving

Hiermee wordt bedoeld of de gegevens correct en actueel zijn. Deelaspecten hiervan zijn:

- **Juistheid**: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd;
- **Volledigheid**: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;
- **Waarborging**: de mate waarin de correcte werking van de IT-processen is gewaarborgd.

Voor de integriteit komt de classificatie respectievelijk overeen met: ***niet noodzakelijk, noodzakelijk, vereist, absoluut***.

Niveau 1: Integriteit is niet noodzakelijk.	**Niveau 2:** Integriteit is noodzakelijk.	**Niveau 3:** Integriteit is vereist.	**Niveau 4:** Integriteit is absoluut.
Blijvende juistheid van informatie (vanaf de bron tot het laatste gebruik) is gewenst, maar hoeft niet gegarandeerd te zijn. Indien informatie niet correct is, leidt dit tot beperkte schade.	*Blijvende juistheid van informatie moet maximaal gewaarborgd zijn. Sommige toleranties zijn toelaatbaar. Juistheid van informatie is belangrijk, maar niet kritisch. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is, kan de organisatie substantiële schade lijden.*	*Informatie moet gegarandeerd correct zijn. Het is echter niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is, kan de organisatie ernstige schade lijden.*	*Informatie moet gegarandeerd correct zijn. Informatie waarbij het noodzakelijk is dat de correctheid niet betwist kan worden, zoals de uitslagen van toetsen, examens, onomkeerbare financiële transacties. Indien informatie niet correct is, kan de organisatie ernstige schade lijden.*
Tussen 0 en 2	Tussen 3 en 7	Tussen 8 en 13	Tussen 14 en 18

3.2 Integriteitsschema

Dit schema moet per toepassing ingevuld worden.

Plaats een ‘x’ in de bijhorende kolom om de classificatie te maken, en motiveer elke vraag. Tel het eindtotaal op om de classificatie van de toepassing te bekomen (zie tabel in § 3.1). *0 staat voor “niet van toepassing”.*

Vragen	**0**	**1**	**2**	**3**	**Motivatie**
Kan er fraude met leerresultaten of financiële fraude plaatsvinden door fouten in de gegevens of ongeautoriseerde wijzigingen? *1 = nee, de gegevens lenen zich bijna niet voor fraude* *2 = beperkt, gegevens worden ook elders gecontroleerd* *3 = ja, de toepassing is de enige met deze gegevens*					

Vragen	0	1	2	3	Motivatie
Hoe erg is het als er fouten of ongeautoriseerde veranderingen in de gegevens zitten? *1 = niet* *2 = het lesgeven wordt belemmerd maar kan wel doorgaan* *3 = het lesgeven kan niet doorgaan, of er is permanent nadeel*					
Hoeveel effect hebben fouten of ongeautoriseerde veranderingen in gegevens? *1 = alleen intern* *2 = intern en mogelijk is een andere partij beïnvloed* *3 = in een hele keten*					
Leiden fouten of ongeautoriseerde veranderingen tot imagoverlies? *1 = nee* *2 = kortstondig imagoverlies* *3 = langdurig imagoverlies*					
Zijn er contractuele of wettelijke verplichtingen voor de integriteit van gegevens? *1 = nee* *2 = ja, deze eisen stelselmatige controle* *3 = ja, deze eisen stelselmatige controle en bewijs van werking (= rapportering)*					
Kunnen er personen negatieve gevolgen ondervinden als gevolg van het niet correct zijn van gegevens? *1 = niet* *2 = eventuele fouten zijn nog te verbe-teren* *3 = fouten veroorzaken ernstige of lang-durige negatieve gevolgen*					

4 Vertrouwelijkheid

4.1 Omschrijving

Hiermee wordt de mate bedoeld, dat de juiste personen en systemen toegang krijgen tot de gegevens in kwestie.

Deelaspecten hiervan zijn:

- **Authenticatie:** *is het proces waarbij je je identiteit gaat bewijzen (ben je wel diegene die je beweert te zijn). Vaak doen we dit door combinatie van een gebruikersnaam en een wachtwoord.*
- **Autorisatie:** *is een proces waarbij onderzocht wordt of je voldoende rechten hebt of toestemming hebt voor hetgeen je wilt doen. Bijvoorbeeld: een leerkracht zal toestemming hebben om in het puntenboek van de klas te schrijven, de leerling mag alleen zijn eigen punten lezen. Enkel de zorgverantwoordelijke en de directie kan in het zorgdossier van een leerling schrijven.*
- **Auditing (Controleerbaarheid):** *is het proces waarmee je kan nagaan wie wat waar, wanneer en waarmee doet. Vaak heb je hiervoor een hulpmiddel nodig dat je kan vertellen wat er op elk moment gebeurde. Dit kan onder meer in de vorm van een logboek.*

Voor de vertrouwelijkheid komt de classificatie respectievelijk overeen met: ***openbaar, intern, vertrouwelijk, geheim***.

Niveau 1: Informatie is openbaar	**Niveau 2:** Informatie is intern	**Niveau 3:** Informatie is vertrouwelijk.	**Niveau 4:** Informatie is geheim.
Openbaar worden van gegevens leidt tot weinig of geen schade voor een instelling of betrokkene.	*De organisatie, instelling of betrokkene kan niet meteen substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen, maar informatie mag wel alleen toegankelijk zijn voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know basis).*	*De organisatie, instelling of betrokkene kan substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag alleen toegankelijk zijn voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know basis).*	*De organisatie, instelling of betrokkene kan ernstige schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag uitsluitend toegankelijk zijn voor een zeer geselecteerde groep personen. Hieronder vallen onder andere bijzondere persoonsgegevens.*

4.2 Vertrouwelijkheidsschema

Hieronder staat de classificatie van categorieën van persoonsgegevens, zoals ze op Don Bosco De Puzzel gehanteerd wordt.

Categorie van persoonsgegevens	**Openbaar**	**Intern**	**Vertrouwelijk**	**Geheim**	**Motivatie**
Gegevens van leerlingen					
Rijksregister			x		*De instelling is gemachtigd om het rijksregisternummer te verwerken, maar mag het niet extern ter beschikking stellen.*
Identificatie		X			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Pasfoto		X			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Contact (school)	x				*Schoolcontactcoördinaten mogen extern gebruikt worden.*
Contact (privé)			x		*Privé contactcoördinaten mogen niet extern gebruikt worden.*
Schoolloopbaan		X			*De instelling heeft deze informatie nodig, maar mag het niet zomaar extern ter beschikking stellen.*
Afwezigheden			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Evaluatie (puntenboeken, rapporten)			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Evaluatie (deliberaties, verslagen)			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*

Categorie van persoonsgegevens	Openbaar	Intern	Vertrouwelijk	Geheim	Motivatie
Functioneren			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Medische informatie				x	*De instelling heeft deze gevoelige informatie nodig, maar dient deze zorgvuldig af te schermen.*
Gegevens van ouder(s) / voogd					
Identificatie		X			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Adres		X			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Contact (privé)			x		*Privé contactcoördinaten mogen niet extern gebruikt worden.*
Financiëel: gegevens bank(rekening)		X			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Financiëel: openstaande schuld				x	*De instelling heeft deze gevoelige informatie nodig, maar dient deze zorgvuldig af te schermen.*
Gegevens van personeelsleden					
Rijksregister			x		*De instelling is gemachtigd om het rijksregisternummer te verwerken, maar mag het niet extern ter beschikking stellen.*
Identificatie		x			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Pasfoto			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Contact (school)	x				*Schoolcontactcoördinaten mogen extern gebruikt worden.*
Contact (privé)			x		*Privé contactcoördinaten mogen niet extern gebruikt worden.*
Loopbaan		x			*De instelling heeft deze informatie nodig, maar mag het niet zomaar extern ter beschikking stellen.*
Afwezigheden			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Financiëel: gegevens bank(rekening)		x			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Financiëel: openstaande schuld				x	*De instelling heeft deze gevoelige informatie nodig, maar dient deze zorgvuldig af te schermen.*
Functioneren en evaluatie				x	*De instelling heeft deze gevoelige informatie nodig, maar dient deze zorgvuldig af te schermen.*
Levensbeschouwing				x	*De instelling heeft deze gevoelige informatie nodig, maar dient deze zorgvuldig af te schermen.*

Categorie van persoonsgegevens	Openbaar	Intern	Vertrouwelijk	Geheim	Motivatie
Gegevens van oud-leerlingen					
Rijksregister		x			*De instelling is gemachtigd om het rijksregisternummer te verwerken, maar mag het niet extern ter beschikking stellen.*
Identificatie		x			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Contact (privé)			x		*Privé contactcoördinaten mogen niet extern gebruikt worden.*
Schoolloopbaan		x			*De instelling heeft deze informatie nodig, maar mag het niet zomaar extern ter beschikking stellen.*
Evaluatie (deliberaties, verslagen)			x		*De instelling dient deze informatie bij te houden, maar niet iedereen dient er toegang toe te hebben.*
Gegevens van oud-personeelsleden					
Rijksregister		x			*De instelling is gemachtigd om het rijksregisternummer te verwerken, maar mag het niet extern ter beschikking stellen.*
Identificatie		x			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Contact (privé)			x		*Privé contactcoördinaten mogen niet extern gebruikt worden.*
Loopbaan		x			*De instelling heeft deze informatie nodig, maar mag het niet zomaar extern ter beschikking stellen.*
Functioneren en evaluatie				x	*De instelling mag deze gevoelige informatie bijhouden, maar dient deze zorgvuldig af te schermen.*

COMMUNICATIEBELEID

Don Bosco Onderwijscentrum

voor:

Don Bosco De Puzzel Haacht

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

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	03/05/2018	GELDIG		

1 Inleiding

De manier waarop personeelsleden, en ook leerlingen en ouders, communiceren maakt ook een deel uit van het IVP-beleid. In dit document worden enkele principes vastgelegd inzake interne én externe communicatie, teneinde er samen voor te zorgen dat de privacy, de informatieveiligheid op en het imago van Don Bosco De Puzzel op een gepast niveau wordt behouden.

Deze nota valt onder de eindverantwoordelijkheid van Don Bosco Onderwijscentrum.

2 Discretieplicht

Alle personeelsleden van Don Bosco De Puzzel zijn gebonden aan een **discretieplicht**, ten aanzien van de persoonsgegevens van leerlingen, ouders of het gezin, en eventueel ten aanzien van elkaars persoonsgegevens. In het *algemeen reglement van het personeel van het katholiek onderwijs* (art. 7 § 7, art. 23 § 1) wordt hiernaar verwezen.

Dit betekent concreet dat zij van ambtswege uit, geen persoonsinformatie mogen vermelden of publiceren, buiten de daarvoor voorziene kanalen binnen Don Bosco De Puzzel. Onderling informatie delen mag natuurlijk, maar dan via de hieronder vastgelegde kanalen en procedures, en steeds indien het in het belang is van het kind, de kinderen of eventueel de collega in kwestie.

Personeelsleden worden dus van ambtswege uit geacht om de geldende beveiligings- en privacyprocedures en -afspraken steeds te volgen, teneinde het **accidenteel** verspreiden van persoonsgegevens te vermijden. Indien men vermoedt dat, door toedoen van uzelf of van anderen, er mogelijks persoonsgegevens buiten de context van deze discretieplicht “geraakt” zijn, dan dient men het aanspreekpunt informatieveiligheid en/of het meldpunt datalekken hierover te contacteren.

Voor Don Bosco De Puzzel is het meldpunt datalekken: ***privacy@depuzzelhaacht.be***.

3 E-mailbeleid

Voor personeelsleden wordt hiernaar verwezen in het arbeidsreglement.

Op Don Bosco De Puzzel maken we onderscheid tussen drie categorieën van emailaccounts:

- Algemene schoolemail (zoals o.a. *info@depuzzelhaacht.be*, *directie@depuzzelhaacht.be*, *leerkrachten@depuzzelhaacht*, …)
- Privé-e-mail (zelf aangemaakt Gmail, Outlook, Live, Yahoo, … account)
- Persoonlijke school- of werk-e-mail (van de vorm *voornaam.naam@depuzzelhaacht.be*)

Voor elk van deze categorieën leggen we in deze paragraaf een aantal richtlijnen / afspraken vast inzake het doel, gebruik én de beveiliging van de accounts in kwestie.

Algemene opmerking: *Verzend nooit een wachtwoord, voor eender welk platform, via e-mail of een ander communicatiesysteem. Niemand van Don Bosco De Puzzel zal op deze manier ooit een wachtwoord opvragen.*

3.1 Algemene accounts

Het beheer hiervan is toegewezen aan één of meerdere medewerkers.

Deze adressen worden vrij verspreid en gepubliceerd.

Indien het adres verwijst naar een groep van personen, dan dient men het steeds in “blind carbon copy” (BCC) te plaatsen.

3.2 Privé-accounts

Deze accounts worden bij voorkeur gebruikt voor niet-school gerelateerde communicatie of handelingen.

Deze adressen worden niet verspreid of gepubliceerd. Ze worden enkel intern gebruikt door directie, administratie of op eigen initiatief.

Het gebruik van dergelijke accounts is niet verboden op Don Bosco De Puzzel, zolang het de professionele bezigheden niet hindert en de informatieveiligheid niet in het gedrang komt.

Concreet:

- Het is niet toegestaan om berichten te verzenden met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud.
- Het is niet toegestaan om berichten te verzenden met een (seksueel) intimiderende inhoud.
- Het is niet toegestaan om berichten te verzenden die (kunnen) aanzetten tot haat en/of geweld.

Gebruik geen privé accounts voor communicatie met collega’s aangaande instellingsgebonden zaken of voor de communicatie met leerlingen, oud-leerlingen, ouders of externen.

Let er bij het gebruik van privé accounts, op toestellen of een netwerk waarop zich ook persoonsgegevens van Don Bosco De Puzzel bevinden, op dat bijlagen, hyperlinks, tools, … die met de privé accounts gebruikt worden, niet leiden tot beveiligingsgevaren zoals virussen, ransomware, phishing[1] enz. Accounts waarmee dergelijke beveiligings-risico’s gedetecteerd worden, zullen steeds geblokkeerd worden.

[1] Meer informatie over “phishing” is te vinden in § 1 van de ***achtergrondinformatie***.

3.3 Schoolaccounts (werkadressen)

Deze zijn telkens toegewezen aan één medewerker en zijn identificeerbaar voor die functie / medewerker.

Deze adressen kunnen verspreid en gepubliceerd worden.

Gebruik deze accounts voor communicatie met collega's aangaande instellingsgebonden zaken of voor de communicatie met leerlingen, oud-leerlingen, ouders of externen.

Natuurlijk gelden dezelfde afspraken voor deze accounts als voor privé accounts:

- Deze accounts worden aan de medewerker voor professioneel gebruik beschikbaar gesteld. Gebruik is derhalve verbonden met taken die voortvloeien uit de functie.
- Beperkt persoonlijk gebruik van deze accounts is evenwel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en dit geen verboden gebruik in de zin van § 3.2 oplevert:

- Het is niet toegestaan om berichten te verzenden met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud
- Het is niet toegestaan om berichten te verzenden met een (seksueel) intimiderende inhoud.
- Het is niet toegestaan om berichten te verzenden die (kunnen) aanzetten tot haat en/of geweld.

Bijkomende afspraken:

- Verzend bij voorkeur **geen gevoelige persoonsgegevens** over leerlingen via deze accounts, of via eender welk ander berichtensysteem (zie ook § 4).
  Dit maakt het voor de verantwoordelijken onmogelijk om iedereens privacy en/of de informatieveiligheid als geheel te waarborgen. Mogelijks leidt dit er toe dat Don Bosco De Puzzel niet alle rechten en vrijheden van leerlingen, ouders of medewerkers kan waarborgen.
  Met gevoelige informatie bedoelen we o.a. gezinssituatie, psycho-sociaal, medisch, zorg, financieel.
  Gebruik het (centraal beheerde en beveiligde) leerlingvolgsysteem om deze informatie met de juiste collega's en medewerkers te delen.
- Indien u via dit emailaccount (gevoelige) persoonsgegevens ontvangt, plaats deze dan zo snel mogelijk in het **(centraal beheerde en beveiligde) leerlingvolgsysteem** of laat een bevoegde medewerker dit er in plaatsen.
  Verwijder daarna alle berichten die deze gegevens bevatten of behandelden (ook uit uw "Prullenmand").
- Gebruik dit account niet op het world wide web, voor platformen die niet nodig zijn om uw taak voor Don Bosco De Puzzel uit te voeren of voor platformen **die niet "informatieveilig" beschouwd worden** door het aanspreekpunt informatieveiligheid. Contacteer voor vragen hierrond *privacy@depuzzelhaacht.be*.
- Maak zo veel mogelijk gebruik van "blind carbon copy" (BCC) indien u met meerdere mensen communiceert.
- Let op wie u bij de ontvangers plaatst of in kopieert, met "carbon copy" (CC).

4 Beleid inzake communicatie-apps

Naast email, zijn er tegenwoordig tal van andere communicatieplatformen, ook op mobiele toestellen. Op Don Bosco De Puzzel moedigen we het (professionele, correcte) gebruik van allerhande tools, platformen en apps natuurlijk aan, maar tegelijkertijd willen we iedereen wijzen op het correcte gebruik ervan, en i.h.b. ten aanzien van privacy-gevoelige informatie.

We menen dat medewerkers, ouders en leerlingen verbonden aan Don Bosco De Puzzel hoofdzakelijk een of meerdere van de volgende communicatieplatformen gebruiken:

- Het berichtensysteem van Iomniwize
- Instant messaging via telefonie, zoals bv. SMS, MMS e.d.
- Instant messaging online, zoals bv. Messenger, WhatsApp, Google Hangouts, …
- Video conferencing, zoals bv. Skype, FaceTime, Google Hangouts, …

4.1 Intern berichtensysteem

Voor het beleid en de regels rond het **interne berichtensysteem**, verwijzen we naar het gebruik van de school email-accounts, zoals beschreven in § 3.3.[2]

Indien Iomniwize een “app” aanbiedt om het interne communicatiesysteem (en eventueel andere functionaliteiten of modules) te raadplegen op een mobiel toestel, vragen wij om dit toestel met een vergrendeling te beveiligen (zie § 5.2 in het ***toestelbeleid***).

4.2 Instant messaging

Deze communicatiekanalen kunnen heel zinvol zijn, ook voor een snel (informeel) werkoverleg, maar binnen Don Bosco De Puzzel is het ten strengste afgeraden om persoonsgegevens van leerlingen te communiceren via een van deze kanalen.

Indien deze kanalen en/of school emailaccounts geraadpleegd worden op een mobiel toestel, vragen wij om dit toestel met een vergrendeling te beveiligen (zie § 5.2 in het ***toestelbeleid***).

4.3 Video conferencing

Ook deze tools zijn zeer interessant, bv. om een overleg van op afstand of met een anders verhinderde collega uit te voeren, maar wees u bewust van:

- de mogelijkheid om in deze tools stem- en/of video-opnames te maken;
- de mogelijkheid om een scherm te delen / over te nemen.

Indien de video conferencing een “app” gebruikt op een mobiel toestel, vragen wij om dit toestel met een vergrendeling te beveiligen (zie § 5.2 in het ***toestelbeleid***).

[2] We wijzen er iedereen via deze weg op dat de beheerders van Iomniwize de berichtinhoud van andere gebruikers onmogelijk kunnen lezen.

5 Social Media-protocol

Bron: https://www.hetstreek.nl/sites/default/files/Protocol%20Sociale%20Media%20%20-%20april%202012.pdf

5.1 Inleiding

Sociale media zoals Twitter, Facebook, LinkedIn, Instagram, Snapchat, … en nog vele anderen bieden de mogelijkheid te laten zien dat men trots is op de school. Tevens kunnen ze een bijdrage leveren aan een positief imago van Don Bosco De Puzzel.

Het is daarbij van belang te beseffen dat berichten op sociale media (onbewust) de goede naam van de school en betrokkenen ook kunnen schaden. Om deze reden vraagt Don Bosco De Puzzel de aan de school verbonden personen om verantwoord met sociale media om te gaan, de reguliere fatsoensnormen in acht te nemen en de mogelijkheden met een positieve instelling te benaderen.

Don Bosco De Puzzel heeft dit protocol opgezet om aan iedereen die betrokken is, of zich betrokken voelt, richtlijnen te geven. Deze richtlijnen maken een effectieve inzet van sociale media mogelijk. Don Bosco De Puzzel is zich bewust van het feit dat de mogelijkheden van sociale media omvangrijk zijn en dat ze bijna dagelijks veranderen. Om enige toekomstvastheid van dit protocol te borgen zijn de richtlijnen zo generiek als mogelijk omschreven, maar wel getoetst op toepasbaarheid in specifieke situaties.

5.2 Uitgangspunten

1. Don Bosco De Puzzel onderkent het belang van sociale media.

2. Dit protocol heeft als doel bij te dragen aan een goed en veilig school- en onderwijsklimaat.

3. Dit protocol bevordert dat indien de school, medewerkers, leerlingen en ouders op de sociale media communiceren, dit gebeurt in het verlengde van de missie en visie van de onderwijsinstelling en de reguliere fatsoensnormen. In de regel betekent dit dat we zorgvuldig communiceren, respect voor de school en voor elkaar hebben en iedereen in zijn waarde laten.

4. Het protocol heeft als doel de onderwijsinstelling, de medewerkers, de leerlingen en de ouders te beschermen tegen de mogelijk negatieve gevolgen van sociale media.

5.3 Doelgroep en reikwijdte

Deze richtlijnen zijn bedoeld voor alle betrokkenen die deel uitmaken van de “schoolomgeving”, dat wil zeggen medewerkers, leerlingen, ouders/verzorgers en mensen die op een andere manier verbonden zijn aan Don Bosco De Puzzel.

De richtlijnen in dit protocol hebben betrekking op alle op enigerlei wijze aan school of haar medewerkers te relateren berichten.

5.4 Sociale media in de school

5.4.1 *Voor alle gebruikers*

1. Het is leerlingen niet toegestaan om tijdens de lessen actief te zijn op sociale media tenzij er op voorhand door de schoolleiding, leraren en/of onderwijsondersteunend personeel toestemming is gegeven.

2. Het is medewerkers toegestaan om tijdens de lessen actief te zijn op sociale media zolang dit een onderwijskundige doelstelling heeft.

3. Het is betrokkenen toegestaan om kennis en informatie te delen, mits het geen vertrouwelijke informatie betreft en andere betrokkenen niet schaadt.

4. De betrokkene is persoonlijk verantwoordelijk voor de inhoud welke hij of zij publiceert op de sociale media.

5. Elke betrokkene dient zich ervan bewust te zijn dat de gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar zullen zijn en kunnen blijven, ook na verwijdering van het bericht. Dat vraagt om extra zorg en enig voorbehoud bij het plaatsen van berichten.

6. Het is niet toegestaan om foto-, film- en geluidsopnamen van school gerelateerde situaties op de sociale media te zetten tenzij de betrokkenen hier uitdrukkelijk toestemming voor hebben gegeven.

7. Op de sociale media waarop geen volledige controle mogelijk is op de berichten die er door anderen worden geplaatst (zoals bv. Facebook) is het medewerkers van Don Bosco De Puzzel afgeraden om privé pagina's en uitingen te delen of het zogenaamde 'vrienden' worden met leerlingen van Don Bosco De Puzzel. De communicatie op deze sociale media vindt plaats via generieke pagina's en profielen (Zie § 5.4.2).

5.4.2 *Voor medewerkers in werksituaties*

1. Indien het wenselijk is dat er voor een bepaald doel een pagina op sociale media wordt aangemaakt, dan wordt hiervoor een generiek, duidelijk aan school gebonden profiel gebruikt. Het aanmaken van een dergelijke pagina wordt op voorhand met de directe leidinggevende besproken.

2. Elke betrokkene is zich bewust van het feit dat (op sommige sociale media) ook anderen informatie kunnen plaatsen op (profiel) pagina's (taggen, linken, posten, etc.).

3. Om die reden zal de eigenaar van de pagina (of topic, discussie, etc.) controlerend optreden en actief redactie voeren op de onder zijn of haar verantwoording aangemaakte pagina's. Zodra de pagina's niet meer nodig zijn worden deze ook door hem of haar weer verwijderd of op non actief gesteld.

4. Medewerkers hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media. Wanneer een medewerker deelneemt aan een discussie of informatie plaatst op een generieke aan school gebonden pagina, dan dient dit in overeenstemming met de officiële standpunten, missie en visie van de onderwijsinstelling te geschieden.

5. Als online communicatie dreigt te ontsporen dient de medewerker direct contact op te nemen met zijn/haar leidinggevende om de te volgen strategie te bespreken.

6. Bij twijfel of een publicatie in strijd is met deze richtlijnen neemt de medewerker contact op met zijn/haar leidinggevende.

5.4.3 *Voor medewerkers buiten werksituaties*

1. Het is medewerkers toegestaan om persoonlijke webpagina's, weblogs, vlogs enz. te onderhouden. Het is daarbij niet toegestaan om aan school gerelateerde onderwerpen te publiceren voor zover het vertrouwelijke of persoonsgebonden informatie over de school, zijn medewerkers, leerlingen, ouders/verzorgers en andere betrokkenen betreft. Een medewerker kan steeds aangesproken worden op berichten, geplaatst op sociale media. Medewerkers moeten zich bewust zijn van hun voorbeeldfunctie.

TOEGANGSMATRICES

Don Bosco Onderwijscentrum

voor:

Don Bosco De Puzzel Haacht

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

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	03/05/2018	GELDIG		

1 Inleiding

1.1 Situering

In deze nota bepalen we het gebruikersrechtenbeleid op Don Bosco De Puzzel Haacht, gebaseerd op de ***classificatie van (persoons)gegevens***. Hiermee bedoelen we dat hier omschreven wordt welke gebruikers(groepen) welke toegangen hebben tot bepaalde gegevens. Hiervoor worden de vertrouwelijkheidsniveau's gehanteerd.

Bepaalde (persoons)gegevens en systemen worden meer specifiek vastgelegd in deze nota, teneinde dit gebruikersrechtenbeleid voldoende gedetailleerd uit te werken.

Deze nota valt onder de eindverantwoordelijkheid van Don Bosco Onderwijscentrum.

1.2 Gebruikersgroepen

Alle dragers, platformen, systemen en het netwerk die binnen Don Bosco De Puzzel Haacht gebruikt worden, vallen onder het IVP-beleid. Dit houdt in het bijzonder in dat elk van deze dragers, platformen, systemen en het netwerk voorzien zijn van **beveiligingsgroepen**, waartoe de respectievelijke gebruikers behoren na authenticatie. (Zie het ***toestelbeleid*** en ***wachtwoordbeleid***.)

De volgende gebruikersgroepen worden hierbij gehanteerd:

- *ICT-coördinatoren*
- *CLB-medewerkers*
- *Directieleden*
- *Zorgverantwoordelijken*
- *Leerkrachten*
  - *Die les geven aan betrokken leerling*
  - *Die geen les geven aan betrokken leerling*
- *Secretariaat*
  - *Die bevoegd zijn om (in welbepaalde zin) leerlinggegevens te verwerken*
  - *Die bevoegd zijn om (in welbepaalde zin) personeelsgegevens te verwerken*
  - *Die hier niet voor bevoegd zijn*
- *Ouder(s) of voogd, stiefouder(s)*
- *Betrokkene zelf*
- *Derden (bv. onderhoudspersoneel, externe betrokkenen)* [1]

Deze groepen worden globaal gehanteerd binnen het IVP-beleid van Don Bosco De Puzzel Haacht. Mogelijks bestaan er, voor welbepaalde gevallen of toepassingen, hiernaast nog specifiekere beveiligingsgroepen.

1.3 Gebruikersrechten

De algemeen gehanteerde gebruikersrechten zijn:

- GT: geen toegang (*men kan de gegevens niet opvragen of zien. Ze worden ook niet in overzichten of dergelijke vermeld*);
- L: leestoegang (*men kan alles zien, maar niets verwijderen, toevoegen of aanpassen*);
- W: wijzig- of schrijftoegang (*men kan alles zien, items toevoegen en aanpassen*)[2];
- D: verwijdertoegang (*men kan alles zien, items toevoegen, aanpassen en verwijderen*);

[1] Hiertoe behoren bv. de medewerkers van externe verwerkers, die in opdracht van Don Bosco De Puzzel Haacht persoonsgegevens ontvangen en/of verwerken.

[2] Mogelijks zijn deze rechten enkel van toepassing op items die door de persoon zelf toegevoegd werden (eigenaarschap) en niet noodzakelijk ook op items van andere gebruikers. Een versiebeheer houdt bij wie wanneer welke aanpassingen aan de inhoud doet.

- VB: volledig beheer (*dit wil zeggen dat men ook de toegangsrechten, van zichzelf en van anderen, kan aanpassen*).

2 Toegangsmatrices

Voor de oplijsting van de concrete gegevens die zich in de hier gehanteerde vertrouwelijkheidsniveau's bevinden: zie de ***classificatie van persoonsgegevens***.

Indien een bepaalde gebruikersgroep niet tot de matrix behoort, hebben deze mensen sowieso geen toegang (GT). Dit noemt men het **privacy by default**-principe.

2.1 Gegevens van leerlingen

<table>
<tr><th></th><th>ICT-coördinatoren</th><th>CLB-medewerkers</th><th>Directieleden</th><th>Zorgverantwoordelijken</th><th>Leerkrachten (les)</th><th>Leerkrachten (geen les)</th><th>Secretariaat (bevoegd)</th><th>Ouder(s), voogd</th><th>Betrokkene zelf</th><th>Derden, externen</th></tr>
<tr><td>Openbaar</td><td colspan="10">Niet van toepassing</td></tr>
<tr><td>Intern</td><td rowspan="3">VB</td><td rowspan="3">L</td><td rowspan="3">L</td><td colspan="3">L</td><td>WD</td><td rowspan="3" colspan="2">GT</td><td rowspan="3">GT</td></tr>
<tr><td>Vertrouwelijk</td><td rowspan="2">WD</td><td>L</td><td rowspan="2">GT</td><td>L</td></tr>
<tr><td>Geheim</td><td>GT</td><td>GT</td></tr>
</table>

Noten; toelichting:

- Ouder(s), voogden en betrokkenen zelf: hebben recht op informatie, inzage en correctie. Dit wil niet zeggen dat ze automatisch toegang tot het leerlingvolg- of leerlingevaluatiesystemen moeten krijgen.

2.2 Gegevens van ouder(s), stiefouder(s) of voogd(en)

<table>
<tr><th></th><th>ICT-coördinatoren</th><th>CLB-medewerkers</th><th>Directieleden</th><th>Zorgverantwoordelijken</th><th>Leerkrachten (les)</th><th>Leerkrachten (geen les)</th><th>Secretariaat (bevoegd)</th><th>Ouder(s), voogd</th><th>Betrokkene zelf</th><th>Derden, externen</th></tr>
<tr><td>Openbaar</td><td colspan="10">Niet van toepassing</td></tr>
<tr><td>Intern</td><td rowspan="2">VB</td><td rowspan="2">L</td><td rowspan="2">L</td><td colspan="3">L</td><td>WD</td><td rowspan="2" colspan="2">GT</td><td rowspan="2">GT</td></tr>
<tr><td>Vertrouwelijk</td><td>WD</td><td>L</td><td>GT</td><td>L</td></tr>
<tr><td>Geheim</td><td colspan="10">Niet van toepassing</td></tr>
</table>

Specifieke rechten; uitzonderingen:

Financiële gegevens	VB	GT	L	GT		WD	GT	GT

Noten; toelichting:

- Financiële gegevens: openstaande rekeningen en afbetalingen hoeven enkel maar door een beperkt aantal bevoegde personen verwerkt te worden.
- Ouder(s), voogden en betrokkenen zelf: hebben recht op informatie, inzage en correctie. Dit wil niet zeggen dat ze automatisch toegang tot de administratieve systemen moeten krijgen.

2.3 Gegevens van personeelsleden

<table>
<tr><th></th><th>ICT-coördinatoren</th><th>CLB-medewerkers</th><th>Directieleden</th><th>Zorgverantwoordelijken</th><th>Leerkrachten (les)</th><th>Leerkrachten (geen les)</th><th>Secretariaat (bevoegd)</th><th>Ouder(s), voogd</th><th>Betrokkene zelf</th><th>Derden, externen</th></tr>
<tr><td>Openbaar</td><td rowspan="4">VB</td><td colspan="5">L</td><td rowspan="4">WD</td><td colspan="3">L</td></tr>
<tr><td>Intern</td><td rowspan="3">GT</td><td rowspan="3">WD</td><td colspan="3" rowspan="3">GT</td><td colspan="3" rowspan="3">GT</td></tr>
<tr><td>Vertrouwelijk</td></tr>
<tr><td>Geheim</td></tr>
</table>

Noten; toelichting:

- Betrokkene zelf: heeft recht op informatie, inzage en correctie. Dit wil niet zeggen dat hij/zij automatisch toegang tot de administratieve systemen moet krijgen, behoudens de openbare gegevens.

2.4 Gegevens van oud-leerlingen

<table>
<tr><th></th><th>ICT-coördinatoren</th><th>CLB-medewerkers</th><th>Directieleden</th><th>Zorgverantwoordelijken</th><th>Leerkrachten (les)</th><th>Leerkrachten (geen les)</th><th>Secretariaat (bevoegd)</th><th>Ouder(s), voogd</th><th>Betrokkene zelf</th><th>Derden, externen</th></tr>
<tr><td>Openbaar</td><td colspan="10">Niet van toepassing</td></tr>
<tr><td>Intern</td><td>VB</td><td>GT</td><td>L</td><td colspan="3">GT</td><td>L</td><td colspan="2">GT</td><td>GT</td></tr>
<tr><td>Vertrouwelijk</td><td colspan="10" rowspan="2">Niet van toepassing
(verwijderd)</td></tr>
<tr><td>Geheim</td></tr>
</table>

Specifieke rechten; uitzonderingen:

Rijksregisternummer	VB	GT					L	GT		GT

Noten; toelichting:

- Bij interne gegevens rekenen we o.a. de wettelijke bewaartermijnen voor leerlinggebonden documenten, o.a. deliberatiebeslissingen, notulen van de klassenraad, enz.

- Ouder(s), voogden en betrokkenen zelf: hebben recht op informatie, inzage en correctie. Dit wil niet zeggen dat ze automatisch toegang tot de administratieve systemen moeten krijgen.

2.5 Gegevens van oud-personeelsleden

<table>
<tr><th></th><th>ICT-coördinatoren</th><th>CLB-medewerkers</th><th>Directieleden</th><th>Zorgverantwoordelijken</th><th>Leerkrachten (les)</th><th>Leerkrachten (geen les)</th><th>Secretariaat (bevoegd)</th><th>Ouder(s), voogd</th><th>Betrokkene zelf</th><th>Derden, externen</th></tr>
<tr><td>Openbaar</td><td colspan="10">Niet van toepassing</td></tr>
<tr><td>Intern</td><td rowspan="3">VB</td><td rowspan="3">GT</td><td rowspan="3">L</td><td colspan="3" rowspan="3">GT</td><td rowspan="3">L</td><td colspan="3" rowspan="3">GT</td></tr>
<tr><td>Vertrouwelijk</td></tr>
<tr><td>Geheim</td></tr>
</table>

Noten; toelichting:

- Betrokkene zelf: heeft recht op informatie, inzage en correctie. Dit wil niet zeggen dat hij/zij automatisch toegang tot de administratieve systemen moet krijgen.

TOESTELBELEID

Don Bosco Onderwijscentrum

voor:

Don Bosco De Puzzel Haacht

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

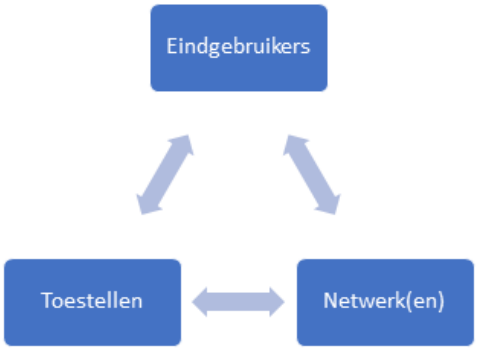
Versie	Datum	Status	Auteur(s)	Opmerking
1.0	03/05/2018	GELDIG		

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



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

Deze nota valt onder de eindverantwoordelijkheid van Don Bosco Onderwijscentrum.

1.2 Algemene bepalingen

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

- Het voorzien van mogelijke manieren om te herkennen wanneer het “gewone” verkeer gemonitord, onderschept, nagebootst of gewijzigd wordt.
- Het mogelijks 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 mogelijks een aantal **identificatieparameters** geregistreerd. Er vinden geen ongeoorloofde inzages 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.

2 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, servers, modems, …

De algemene maatregelen (zie § 1.2) worden toegepast, met i.h.b. mogelijke 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 indien mogelijk aan alle afspraken uit het ***wachtwoordbeleid***.

2.2 Wifi-netwerk *#in*

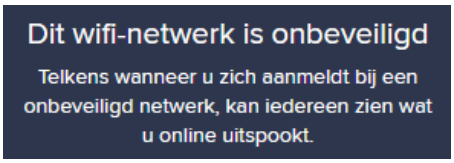
Voor personeel en gasten is wifi voorzien op Don Bosco De Puzzel. Deze dienst is gratis voor de eindgebruikers, maar heeft voor de school wel een zekere kostprijs (in aanschaf, onderhoud en beveiliging).

Daarom wordt mogelijks de aard en hoeveelheid van het netwerkverkeer gemonitord.

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

Ook de bezochte websites of applicaties, en het datagebruik via het draadloze netwerk, kunnen worden 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 Don Bosco De Puzzel 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 Don Bosco De Puzzel 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. mogelijks logging van: tijdsregistratie, MAC- en IP-adressen, toestelnamen, gebruikersnamen.

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

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 mogelijks, 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 Don Bosco De Puzzel dan ook verschillende maatregelen genomen om dit te verhinderen. Het doelbewust veranderen van systeem- of beveiligingsinstellingen is verboden.

Dit beleid wordt mogelijks 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. mogelijks logging van: tijdsregistratie, MAC- en IP-adressen, gebruikersnamen, toestelnamen, logintijd, gebruikte toepassingen, wijzigingen in systeeminstellingen.

- Op Don Bosco De Puzzel kunnen er bepaalde tools gebruikt worden die de actieve vensters en/of het realtime beeldscherm van de eigen toestellen kunnen monitoren. De doeleinden hiervan zijn louter en alleen pedagogisch. Het is i.h.b. leerkrachten en ondersteunend personeel *niet* toegestaan om zonder concreet vermoeden van doelbewuste en ernstige inbreuken, schermafdrukken te bewaren, een scherm op te nemen of een scherm over te nemen zonder toestemming van de betrokkene.

- Leerkrachten en ondersteunend personeel kunnen, in het kader van hun uit te oefenen taak, de actieve vensters, 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 medewerkers 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 kunnen 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 Don Bosco De Puzzel, 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:

- Encryptie van opslagmedia (indien mogelijk);
- Optie om te lokaliseren of te wissen van op afstand, in geval van diefstal of verlies (indien mogelijk)

5 Beveiliging en controle op toestellen van eindgebruikers zelf

Op Don Bosco De Puzzel 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 Don Bosco De Puzzel, 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]-beleid, zijn:

Het internetverkeer en gebruikte toepassingen wordt mogelijks, 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. mogelijks logging van: MAC- en IP-adressen, gebruikersnamen, toestelnamen, logintijd, gebruikte toepassingen, wijzigingen in systeeminstellingen, enz.

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

De mobiele toestellen (d.w.z. laptops, pda's, tablets, smartphones) van medewerkers, waarop persoonsgegevens van Don Bosco De Puzzel 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.
- Back-ups 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:

- Encryptie van opslagmedia (indien mogelijk);
- 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.

WACHTWOORDBELEID

Don Bosco Onderwijscentrum

voor:

Don Bosco De Puzzel Haacht

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

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	03/05/2018	GELDIG		

1 Inleiding

Een goed beveiligingsbeleid is tegenwoordig noodzakelijk voor elke school. Steeds meer privacygevoelige gegevens worden (online) gedeeld en een zwak beveiligingsbeleid zorgt ervoor dat je de deur openzet voor duidelijke risico's. Een goed beveiligingsbeleid geeft gebruikers (leerkrachten, leerlingen, CLB-medewerkers…) toegang tot alle informatie die ze nodig hebben om hun taak naar behoren uit te oefenen maar ontzegt hen alle toegang tot informatie die ze niet nodig hebben.

Er zijn drie pijlers waarop een goed beveiligingsbeleid berust: **authenticatie**, **autorisatie** en **auditing**.

Authenticatie is het proces waarbij je je identiteit gaat bewijzen (ben je wel diegene die je beweert te zijn). Vaak doen we dit door combinatie van een gebruikersnaam en een wachtwoord.

Autorisatie is een proces waarbij onderzocht wordt of je voldoende rechten hebt of toestemming hebt voor hetgeen je wilt doen. Bijvoorbeeld: een leerkracht zal toestemming hebben om in het puntenboek van de klas te schrijven, de leerling mag alleen zijn eigen punten lezen. Enkel de zorgverantwoordelijke en de directie kan in het zorgdossier van een leerling schrijven.

***Auditing* (*Controleerbaarheid*)** is het proces waarmee je kan nagaan wie wat waar, wanneer en waarmee doet. Vaak heb je hiervoor een hulpmiddel nodig dat je kan vertellen wat er op elk moment gebeurde. Dit kan onder meer in de vorm van een logboek.

In dit document zullen we ons beperken tot de authenticatie en in het bijzonder het gebruik van wachtwoorden en andere, bijkomende authenticatiemethodes op Don Bosco De Puzzel.

Deze nota valt onder de eindverantwoordelijkheid van Don Bosco Onderwijscentrum.

2 Toegangsbeheer

De directeur van de school is verantwoordelijk voor het gebruikersbeheer van de organisatie. Gebruikersbeheer houdt het aanmaken van gebruikers, toekennen van rechten en stopzetten van rechten in. Dit betekent dat er in de school een inventaris moet opgezet worden die het overzicht houdt van alle rollen en rechten gekoppeld aan personeelsleden in de school. Het opzetten van een dergelijke procedure rond het toegangsbeheer is belangrijk om de controle te kunnen houden op alle gebruikers die er zijn in de organisatie. Dit is de eerste stap in het authenticatiebeleid.

3 Authenticeren

Er zijn verschillende manieren om je in systemen te authenticeren. De meest gebruikte vorm is de combinatie van een gebruikersnaam en een wachtwoord. Een ander voorbeeld is het gebruik van je bankkaart en je pincode waarmee je je aan een bankautomaat kan authenticeren. Maar ook een vingerafdruk of een irisscan kan gebruikt worden om te kijken of je wel diegene bent die je beweert te zijn.

Wachtwoorden zorgen er mee voor dat de toegang tot applicaties goed beveiligd is. Het is dus van belang om een sterk beleid op te zetten om het inlogproces en -procedures te beheren. Op Don Bosco De Puzzel werken we er continu aan om leerkrachten en leerlingen het belang van sterke wachtwoorden bij te brengen.

Een wachtwoordbeleid heeft als doel enkele bepalingen op te leggen rond het correct gebruik van wachtwoorden om de toegang tot gevoelige data (waaronder privacy gevoelige persoonsgegevens) te beveiligen middels een wachtwoord.

Een sterk wachtwoord is moeilijker te achterhalen en dus veiliger dan een 'zwak' wachtwoord. De sterkte van een wachtwoord hangt af van de lengte, complexiteit en de onvoorspelbaarheid.

3.1 Wachtwoordbepalingen

- Hoe langer een wachtwoord hoe beter. Het wachtwoord moet minstens 12 karakters hebben. (*Tegenwoordig zijn 8 karakters heel snel te raden.*)
  Beter nog is om te werken met een wachtwoordzin (bijv: `IkGaSinds2015NaarDeSchool`)
- Mix hoofdletters, kleine letters en tekens door elkaar: gebruik volgende tekens in het wachtwoord:
  - Hoofdletters
  - Kleine letters
  - Cijfers
  - Niet-alfanumerieke karakters

  Bijv. `P@dd€nsto€l579`

- Gebruik de hoofdletters en andere karakters best niet in het begin van het wachtwoord/wachtzin en wissel ze met elkaar af. Bijv. `p@dd€NSto€l579`
- Keer woorden om. Bijv. `l€otSN€dd@p579`
- Maak wachtwoorden/wachtzinnen die enkel betekenis hebben voor jou.
- Verander minstens één keer per schooljaar je wachtwoord.
- Gebruik verschillende wachtwoorden voor verschillende applicaties; hergebruik je wachtwoord niet!
- Indien de ICT-dienst een wachtwoord instelt of “reset” (zie ook § 3.5) voor een bepaald platform of voor het netwerk, dan zal de gebruiker dit steeds moeten veranderen naar een persoonlijk wachtwoord, bij de eerste aanmelding.

Gebruik een online tool om te zien hoe sterk jouw wachtwoord is: bijv. https://veiliginternetten.nl/wachtwoord-check

3.2 Afraders

- Gebruik geen voor de hand liggende namen, woorden of getallen.
  Bijv. `NaamVoornaamGeboortedatum` of `StraatnaamNr`
- Schrijf het wachtwoord niet op: niet op papier, niet elektronisch in jouw GSM of PC. Bewaar ze zeker niet op een Post-it aan de computer.
  - Indien je toch liefst je wachtwoord opschrijft, bewaar het dan ver van de gebruiker en schrijf er niet bij voor welke applicatie het dient.
- Geef het wachtwoord niet door, op geen enkele wijze aan niemand (ook niet aan iemand van ICT).
- Verzend nooit een wachtwoord via e-mail of een ander communicatiesysteem. (Niemand van Don Bosco De Puzzel zal ooit je wachtwoord, om eender welke reden, op deze manier opvragen.)
- Zorg dat niemand op je vingers kijkt bij het ingeven van een wachtwoord.
- Er is soms de optie om een wachtwoord (even) te tonen, zodat je typfouten kan controleren. Zorg dat er niemand meekijkt op het moment dat je dit gebruikt.
- Besteed bijzondere aandacht aan een externe projectie indien dat aangesloten is, zoals bv. een beamer of (groot) tweede scherm.
- Gebruik geen woord uit het woordenboek.
- Herhaal niet te veel karakters of nummers (bijv. `11223344`).
- Gebruik geen te makkelijke wachtwoorden (bijv. `NaamAchternaamGeboortejaar`, `azertyuiop`).
- Bewaar je wachtwoord niet in de browser.
- Maak geen gebruik van de functie om ingelogd te blijven in een bepaalde applicatie.
- Gebruik andere wachtwoorden dan privé-wachtwoorden.

3.3 Wachtwoordbeheer

- Het is mogelijk dat na een aantal pogingen om in te loggen het account vergrendeld wordt. Neem contact op met de dienst ICT om het account terug te ontgrendelen.
- Laat de computer nooit onbeheerd achter maar vergrendel het scherm of log uit.
- Er kan automatisch gecontroleerd worden op het gebruik van goede wachtwoorden.

3.4 Wat doen bij vermoeden van misbruik?

Misbruik kan ontvreemding of onrechtmatig gebruik van een wachtwoord zijn.

- Verander het wachtwoord onmiddellijk
- Neem direct contact op met het aanspreekpunt informatieveiligheid, de dienst ICT en/of de systeembeheerder. Meldpunt datalekken: privacy@depuzzelhaacht.be

Deze personen gaan na of er sprake is van een misbruik en proberen zo nodig de schade te herstellen.

3.5 Wat doen indien het wachtwoord vergeten werd

- Blijf niet proberen; na een aantal pogingen kan je account vergrendeld worden (zie § 3.3)
- Indien het platform over deze mogelijkheid beschikt, kan je de “wachtwoord vergeten”-optie gebruiken. Meestal zorgt dit ervoor dat er een link gestuurd wordt naar een vooraf ingesteld “back-up” emailadres, waarmee men een nieuw wachtwoord kan instellen (zonder het vorige te kennen).
- Anders neem je persoonlijk contact op met de dienst ICT en/of de systeembeheerder. Zij zullen een tijdelijk wachtwoord instellen (d.i. een “wachtwoordreset”) waarmee de gebruiker terug kan aanmelden.

3.6 Gebruik van wachtwoordmanagers of een wachtwoordkluis

Indien je te veel wachtwoorden moet onthouden, kan je gebruik maken van een wachtwoordkluis. Wachtwoord-kluizen slaan al de wachtwoorden versleuteld op in een beveiligd bestand. Dit bestand wordt geopend met één sterk wachtwoord. Dit wil zeggen dat er maar één wachtwoord meer nodig is om alle wachtwoorden veilig te ontsleutelen.

De volgende wachtwoordkluizen werden veilig bevonden voor onze school:

- KeePass (http://keepass.info/)
- LastPass (https://lastpass.com/nl/)
- Dashlane (https://www.dashlane.com/)
- 1Password (https://agilebits.com/onepassword)
- Passwordsafe (https://www.pwsafe.net/)

4 Gebruik van two-factor authenticatie

Indien je echt met veel privacygevoelige persoonsgegevens werkt, is vaak een combinatie van gebruikersnaam en wachtwoord niet voldoende veilig. De gebruikersnaam is meestal gekend en een wachtwoord kan eventueel gestolen of ontfutseld worden. Daarom bestaan er two-factor authenticatiemethodes.

Een voorbeeld: Naast het gebruik van een gebruikersnaam en wachtwoord krijg je op je gsm een beveiligingscode doorgestuurd die je dan extra moet ingeven vooraleer je toegang krijgt. Naast het weten van de gebruikersnaam en wachtwoord is het dus ook nodig dat je iets in je bezit hebt, zoals bijvoorbeeld een telefoon waar men via sms een code doorgestuurd krijgt.

Deze systemen zijn veel veiliger en worden binnen Don Bosco De Puzzel dan ook aangeraden voor iedereen die aan de meest privacygevoelige gegevens binnen de onderwijsinstelling kan. Concreet denken we hierbij aan iedereen die toegang heeft tot *geheime* gegevens (zie ***classificatie van gegevens*** en de ***toegangsmatrices***).

5 Risico's

Aan een slecht wachtwoordbeleid zijn risico's verbonden. Met dit beleid willen we onderstaande risico's verkleinen en/of uitschakelen.

- **Identiteitsdiefstal:** iemand die jouw wachtwoord achterhaalt, kan zich binnen de systemen in kwestie voordoen met jouw identiteit. Alle handelingen die men met jouw account stelt, kunnen via logging teruggebracht worden naar uzelf en niet naar diegene die met uw digitale identiteit aan de haal ging.

- **Phishing:** via phishing proberen oplichters achter persoonlijke gegevens/wachtwoorden te komen, meestal via e-mail of telefoon. Met deze informatie kunnen oplichters persoonlijke gegevens stelen en publiceren.

  Zie ***Achtergrondinformatie*** – § 1 voor meer informatie rond "phishing".

- **Hacking:** door zwakke wachtwoorden wordt het zeer eenvoudig om in te breken in de informatiesystemen. Eens binnen in het systeem kan er zeer veel schade berokkend en kunnen gegevens gestolen worden.

Rond deze risico's worden alle personeelsleden, maar zeker ook de leerlingen en ouders, binnen Don Bosco De Puzzel actief en herhaaldelijk gesensibiliseerd.

O.a. via Safe on Web kan er veel praktisch materiaal gevonden worden rond dit beleid en rond de hier vermelde risico's:

https://www.safeonweb.be/nl/home