Handboek/gedragscode

Informatiebeveiliging en Privacy (IBP)
en **gebruik digitale media.**

Inhoud

1. Inleiding

In onze huidige sterk digitaliserende maatschappij groeit het aantal beschikbare digitale middelen snel. Ook binnen ons onderwijs worden er steeds meer van deze digitale middelen ter verrijking of aanvulling gebruikt. Met dit toenemend gebruik wordt aandacht voor en afspraken over verantwoordelijk gebruik steeds belangrijker, alsmede het waarborgen van de privacy van onze leerlingen en medewerkers.

Dit handboek is de praktische invulling van het door stichting KBA Nw West geformuleerde beleid op het gebied van Informatiebeveiliging en Privacy. Hiermee bieden we onze medewerkers handvatten om op een verantwoorde manier gebruik te maken van de beschikbare digitale middelen ter verrijking van het onderwijs, waarbij de privacy van alle betrokkenen optimaal is gewaarborgd.

2. Privacy in de wet

Sinds 1983 is privacybescherming opgenomen in de Nederlandse Grondwet. De regelgeving rond privacy is uitgewerkt in de Wet bescherming persoonsgegevens (WBP) en vanaf mei 2018 in de Algemene verordening gegevensbescherming (AVG). De wet beschermt de privacy door regels te stellen voor de omgang met persoonsgegevens in Nederland (WBP) en Europa (AVG). Het uitgangspunt van de wet is dat privacy altijd wordt gerespecteerd. Leerlinggegevens zijn ook persoonsgegevens. De wet is hierop dus van toepassing. Binnen de organisatie is het bevoegd gezag eindverantwoordelijk voor de bescherming van privacy van medewerkers, leerlingen en ouders. Echter alle betrokkenen zijn verplicht om volgens de wet te handelen en daarbij zorgvuldig te werk te gaan. De wet biedt scholen en organisaties voldoende ruimte om binnen de kaders persoonsgegevens te gebruiken.

2.1 Werken met persoonsgegevens: 5 vuistregels

Om persoonsgegevens te mogen verwerken kent de Wet bescherming persoonsgegevens een aantal uitgangspunten. Deze voorwaarden gelden voor elke school/organisatie en zijn samengevat tot 5 vuistregels:

1. **Doel en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk voorafgaand aan de verwerking omschreven en gerechtvaardigde doeleinden. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie**: de persoonsgegevens die de school verwerkt, moeten redelijkerwijs nodig zijn om het doel te bereiken. De gegevens moeten in verhouding staan tot het doel. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie**: de betrokkene (medewerker, leerling en/of zijn ouders) is vooraf in begrijpelijke taal geïnformeerd over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is. Verder hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit**: Maatregelen om te waarborgen dat te verwerken Persoonsgegevens juist en actueel zijn.

2.2 Aanwezige bovenschoolse beleidsdocumenten vanuit wettelijke kaders.

1. Protocol IBP beleid Stichting KBA Nw West
2. Handboek IBP waarin gedragscode en de praktische invulling van het IBP beleid .
3. Een privacyreglement verwerking persoonsgegevens.
4. Een protocol Datalekken inclusief meldingsformulieren.

3. Afspraken rond IBP en gebruik digitale media

3.1 Algemene uitgangspunten:

a. Medewerkers en leerlingen van stichting KBA Nw West kunnen in ruime mate gebruik maken van diverse beschikbare digitale middelen.
b. Medewerkers kunnen voor hun werk gebruik maken van een door de organisatie beheerde laptop/pc. Als werk- en opslagomgeving kunnen medewerkers gebruik maken van een cloudomgeving Office 365. Deze wordt in kalenderjaar 2018 verder geïmplementeerd, zodat medewerkers een betrouwbaar en werkbaar alternatief hebben voor mobiele datadragers.
c. Met de netwerkbeheerder zijn op stichtingsniveau afspraken gemaakt over welke toegangen medewerkers en leerlingen hebben met betrekking tot digitale media en online middelen.
d. Door heldere afspraken en gedragsregels (vastgelegd in verschillende documenten) beschermen we de privacy van medewerkers en leerlingen.
e. Bij keuze, aanschaf en uitbreiding van apparatuur en het vaststellen van procedures is beveiliging en privacybescherming een vast aandachtspunt. Stichting KBA Nw West neemt alleen apparatuur en licenties af bij bedrijven die in staat zijn een bewerkersovereenkomst te overleggen die in lijn is met het landelijk vastgestelde PrivacyConvenant.
f. De leidinggevende is verantwoordelijk voor toezicht, toepassing en controle van gemaakte en vastgelegde afspraken. Meestal is dit de schooldirecteur.

3.2 Afspraken/gedragscode gebruik digitale media

3.2.1 Gebruik apparaten en netwerkvoorzieningen

a. Medewerkers, leerlingen en andere gebruikers mogen door stichting KBA Nw West beschikbaar gestelde digitale middelen ook voor persoonlijke doeleinden gebruiken mits dit niet storend is voor de dagelijkse werkzaamheden en het (computer)netwerk.
b. Van medewerkers, leerlingen en andere gebruikers die via door stichting KBA Nw West beschikbaar gestelde digitale middelen gebruik maken van software, internet, wifi en sociale media verwachten we dat ze hiermee op een integere, correcte wijze omgaan.
c. Ook bij het gebruik van beschikbaar gestelde apparatuur verwachten we van alle gebruikers dat zij netjes en correct met deze middelen omgaan.

3.2.2 BringYourOwnDevice (BOYD): gebruik van eigen apparaten

Scholen bepalen zelf of ze al dan niet het gebruik van eigen ict apparaten (laptop, tablet, telefoon) toestaan. Ook hier geldt dat gebruik van (eigen) apparatuur nooit verstorend mag werken op de dagelijkse schoolwerkzaamheden en het schoolnetwerk.

Als scholen er voor kiezen deze middelen (privé eigendom) ook in te zetten bij hun onderwijs, kan dit alleen op vrijwillige basis waarbij de gebruiker altijd verantwoordelijk blijft voor zijn of haar device.

Hierbij geldt het volgende:

a. Met ouders/verzorgers worden afspraken gemaakt over de aansprakelijkheid bij verlies/diefstal en defecten bij gebruik op school. Hierbij is uitgangspunt dat de school toestemming geeft om het device te gebruiken, maar niet verantwoordelijk en aansprakelijk is voor het device.
b. De school kan leerlingen /medewerkers nooit verplichten om eigen apparaten op de school te gebruiken.
c. Als op de school eigen apparaten zijn toegestaan bepaalt de leerkracht op welke momenten en waarvoor deze apparaten mogen worden gebruikt.

d. De beveiligde draadloze WiFi-netwerkverbinding wordt niet gedeeld met anderen dan uitsluitend personeel of leerlingen.
e. Omdat eigen apparaten geen onderdeel uitmaken van de beheerde schoolomgevingen moet rekening gehouden worden met een doorgaans lager beveiligingsniveau en minder functionaliteit dan op de schoolapparatuur.
f. Voor gebruik van eigen apparaten in de onderwijs/schoolomgeving gelden verder uiteraard dezelfde gebruiks- en gedragsregels als wanneer er vanaf schoolapparaten wordt gewerkt.

3.2.3 Gebruik e-mailgebruik

a. Werknemers mogen hun school-mailbox gebruiken voor alle mail die werkgerelateerd is.
b. We verwachten van onze medewerkers dat ze werkgerelateerde mail alleen via dit mailadres versturen en niet via privé-mailboxen.
c. Hoog privacygevoelige informatie wordt op een zo veilig mogelijke manier uitgewisseld, met inachtneming van de vijf vuistregels. Als via de mail bijlages (met hoog privacygevoelige inhoud) verstuurd worden, worden deze bij voorkeur met een code beveiligd. Deze code kan naar de ontvanger gestuurd worden zodat alleen hij of zij de inhoud zichtbaar kan maken.
d. De mailbox is niet bedoeld als archief voor bijvoorbeeld via de mail ontvangen bijlages. Sla deze altijd op op de daar voor bedoelde opslagomgeving. (zie punt 3.4 van dit document)
e. Bij mail verstuurd naar grote groepen personen gebruiken we bij voorkeur de BCC-functie. Voor interne groepen gebruiken we daarbij de in Office 365 aanwezige distributielijsten.
f. De optie ‘allen beantwoorden’ gebruiken we alleen indien de noodzaak daarvoor aanwezig is.
g. Bij e-mailgebruik stellen we ons eerst de vraag: “Is e-mail het juiste medium voor de inhoud van het te versturen bericht?”
h. Niemand mag, zonder gegronde redenen en toestemming van de eigenaar, de inhoud van een persoonlijke mailbox lezen. Indien er gegronde redenen zijn en er toestemming is namens het CvB, mag de mailbox geopend worden door daarvoor aangewezen en geautoriseerde medewerkers. Hierbij geldt dan dat alleen zakelijke mail bekeken mag worden en dat een eventuele map “privé” niet mag worden ingezien.

3.2.4 Gebruik internet en Sociale Media

a. Bij digitale communicatie (bijvoorbeeld via sociale media) maken medewerkers duidelijk of zij op persoonlijke titel of namens de school publiceren. Sociale media op schoolniveau wordt beperkt gebruikt (afgeschermd) en valt altijd onder het directe beheer (en daarmee de verantwoordelijkheid) van de school. Sociale media-kanalen worden dan ook niet beheerd door ouders of derden.
b. Bij gebruik van sociale media zijn medewerkers van stichting KBA Nw West zich bewust van het feit dat zij vertegenwoordiger zijn van hun school en stichting KBA Nw West.
c. We gaan bewust om met wat we delen op sociale media: Is het wel of niet verstandig te publiceren, wat zijn de eventuele consequenties en is het betreffende sociale platform/middel wel het meest geschikt voor de te delen inhoud. Tenzij het om promotionele doeleinden gaat, wordt daarom een afgeschermde omgeving gebruikt.
d. Medewerkers gaan over school/organisatie gerelateerde onderwerpen niet in discussie op sociale media.
e. Medewerkers van de school publiceren of delen geen vertrouwelijke informatie, zoals persoonsgegevens, foto- of beeldmateriaal van collega’s of leerlingen op persoonlijke sociale media.
f. Onze medewerkers zijn persoonlijk verantwoordelijk voor wat zij publiceren.
g. Foto’s en filmpjes waarop leerlingen herkenbaar staan, mogen uitsluitend gepubliceerd worden als de ouders/verzorgers van de desbetreffende leerlingen hiermee akkoord zijn. Scholen vragenvoor verschillende door de school gebruikte media hiervoor toestemming aan de ouders/verzorgers en wijzen ouders jaarlijks op het feit dat zij deze toestemming kunnen herzien. Dit geldt ook voor het verspreiden van privacygevoelige gegevens zoals die staan op adres- en bellijsten.

h. Onze scholen houden zich bij alle digitale en andere publicaties aan de geldende wettelijk kaders.
i. Om onze leerlingen qua content in een zo veilig mogelijke omgeving te laten werken besteedt elke school bewust aandacht aan het gebruik van sociale media, de gevolgen van het gebruik en de mogelijke acties en reacties aan de hand van voorbeelden.
j. De school zorgt ook digitaal voor een veilig klimaat en communiceert met medewerkers, leerlingen en ouders hoe zij dit doet. (Mediawijsheid)
k. De schoolwebsite is in eerste instantie bedoeld als professioneel informatiemedium voor zowel de ouders/verzorgers van de huidige als toekomstige leerlingen. Daarnaast is op de website altijd de contactinformatie en de contactpersoon van de school vindbaar. Elke schoolwebsite heeft een SSL-certificaat, welke te herkennen is aan de https://-url.

3.2.5 Monitoring en controle > Naast raamovereenkomst netwerkbeheer

a. Controle op het internet- en mailgebruik vindt slechts ten behoeve van onderstaande doelen plaats:
    - Het tegengaan van virussen en andere schadelijke programma's.
    - Het oplossen van netwerk problemen (capaciteit en blokkades etc)
    - Het tegengaan van verboden of foutief gebruik.
b. Controle vindt incidenteel of steekproefsgewijs plaats op het niveau van getotaliseerde en gegevens die niet herleidbaar zijn tot individuele personen. Indien er aanwijzingen of vermoedens zijn dat de regels worden overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden.
c. Controle beperkt zich in principe tot verkeersgegevens van het gebruik van e-mail en internet. Alleen bij zwaarwegende redenen vindt er controle op de inhoud plaats.
d. De leidinggevende spreekt medewerkers en leerlingen, op hun gedrag aan als zij zich niet houden aan de gemaakte afspraken.

~~3.3~~Afspraken gegevensuitwisseling met andere instanties en scholen

3.3

De scholen van stichting KBA Nw West maken gebruik van het leerling administratie systeem ParnasSys. Hiermee vinden de volgende uitwisselingen plaats.

- Tussen scholen onderling van onderwijskundige rapporten en overdrachtsdossiers gebeurt via 'Onderwijs Overstap Service'(OSO).
- De verzuimregistratiemeldingen naar de leerplichtambtenaar~~,~~
- De uitwisseling met DUO en Bron wordt uitsluitend gedaan via het Leerling Administratie Systeem.
-
- De digitale overdracht naar andere instanties zoals bijvoorbeeld zorgaanbieders en de inspectie voor het Onderwijs.

Alle uitwisselingen, met uitzondering van het laatste punt, verlopen via een beveiligd, digitaal portaal met in achtneming van de privacyregels en daarbij horende procedures. Uitgangspunt is ook daar de 5 vuistregels genoemd eerder in dit handboek.

3.4 Afspraken apparaat gebruik en data opslag

Om ervoor te zorgen dat de privacy~~-~~gevoelige informatie zowel binnen als buiten de school beschermd is, hanteren we de volgende afspraken:

a. Medewerkers laten apparaten waarop toegang verkregen kan worden tot privacy~~-~~gevoelige gegevens niet onbeheerd en onbeveiligd achter. Zij kunnen dit doen door af te sluiten, uit te loggen of te vergrendelen. Dit geldt ook voor externe (eigen) apparaten zoals bijvoorbeeld tablets, mobiele telefoons of thuiscomputers.~~-~~

b. Externen hebben als basisregel geen toegang tot leerling-administratie en het leerlingvolgsysteem of enig ander systeem waar (hoog)privacy-gevoelige informatie benaderbaar is.
c. Medewerkers zijn verplicht om zorgvuldig met hun wachtwoorden om te gaan. Dit geldt in het bijzonder voor de (netwerk)inloggegevens en software-pakketten waarin zich persoonsgegevens bevinden. (zie punt 3.5 wachtwoordbeleid).
d. Digitaal versturen van privacygevoelige gegevens dient, daar waar mogelijk, versleuteld of beveiligd te gebeuren.
e. Stichting KBA Nw West gebruikt voor dataopslag als centrale plaats twee eigen omgevingen*:
    - Het netwerk van de stichting, uitgerold door netwerkleverancier De Rolf Groep.
    - Een Office 365 omgeving met Sharepoint, geïmplementeerd door De Rolf Groep.
f. Gebruikers slaan privacy gevoelige data altijd op op de daarvoor aangewezen opslag omgeving van de school of stichting. Hoog privacy gevoelige informatie komt primair in het Leerling Administratie Systeem.
g. Het is niet toegestaan om hoog privacy–gevoelige data op te slaan buiten de daarvoor bedoelde school(Cloud)omgeving. Zeker niet op de lokale harde schijf van de computer of onbeveiligde opslagmiddelen zoals een externe harde schijf, geheugenkaart of USB–stick.

3.5 Wachtwoordbeleid

a. We gaan er van uit dat medewerkers zorgvuldig met hun wachtwoorden om-gaan. Dat betekent o.a. dat wachtwoorden naar omgevingen waar zich privacy-gevoelige data bevindt nooit gedeeld worden met andere personen. Het zichtbaar ophangen van persoonlijke wachtwoorden is niet toegestaan.
b. In de systemen waar stichting KBA Nw West zelf het wachtwoordbeleid kan bepalen en waar privacy gevoelige data wordt opgeslagen (wordt periodiek (minimaal jaarlijks) afgedwongen dat medewerkers een nieuw sterk wachtwoord kiezen. Ook worden accounts in die omgevingen automatisch uitgelogd als deze langere tijd ongebruikt ingelogd zijn op een apparaat. Ook in andere systemen raden we gebruikers aan regelmatig hun wachtwoord te vernieuwen.
c. We gaan m.b.t. wachtwoordeisen en gebruik uit van drie basisregels:
    - Je wachtwoord nooit delen, dat is iets van jou.
    - Je wachtwoord mag niet makkelijk te raden zijn (bijvoorbeeld Mijn kat is lief en niet groen!)
    - Je wachtwoord niet hergebruiken.

3.6 Afspraken bij datalekken

a. Als er door verlies of diefstal van of inbraak in apparatuur (ook usb stick of externe harde schijf) of Cloud omgeving mogelijk sprake is van verlies, onrechtmatig gebruik van of inzage in privacy gevoelige data, spreken we van een (mogelijk) datalek. Bij kennis hiervan is de medewerker verplicht dit aan zijn leidinggevende te melden, zodat de organisatie hier de juiste acties op kan ondernemen.
b. Bij melding van een mogelijk datalek volgen we de procedures zoals die zijn vastgelegd in het ‘Protocol datalekken Stichting KBA Nw West’.

3.7 Afspraken gebruik software en bewerkersovereenkomsten.

Al onze systemen en opslag bevinden zich in Cloud omgevingen. Dat betekent concreet dat de informatie van onze medewerkers en leerlingen zich in de digitale omgevingen van diverse externe partijen bevindt. Basisregel hierbij is dat alle gegevens in deze systemen eigendom zijn van de school/organisatie.

Voor alle softwaresystemen en apps die we gebruiken (dus ook educatieve software en apps) geldt dat zodra er privacy-gevoelige data wordt ingevoerd bovenschools een bewerkersovereenkomst met de leverancier van de software afgesloten moet zijn/worden.

Bij Stichting KBA Nw West dragen we er zorg voor dat die ondertekende bewerkersovereenkomsten aanwezig zijn van de partijen waar wij gegevens opslaan en waarmee we gegevens uitwisselen.

Uitgangspunten bij gebruik van systemen en data invoer zijn:

a. We voeren alleen persoonsgegevens in in systemen/programma's als dit voor het doel noodzakelijk is.
b. Als er i.p.v. persoonsgegevens ook geanonimiseerde gegevens kunnen worden gebruikt heeft dat de voorkeur.
c. Als het noodzakelijk is dat er in systemen/programma's privacy-gevoelige data wordt opgeslagen moet er altijd een bewerkersovereenkomst met de externe partij zijn of z.s.m. komen.
d. Als scholen of medewerkers systemen in gebruik nemen waar privacy-gevoelige data ingevoerd moet worden (persoonsgegevens) checken zij of hiervoor al een bewerkersovereenkomst bij stichting KBA Nw West aanwezig is. Indien dit niet het geval is, kan in overleg met de Functionaris Gegevensbescherming bij de betreffende leverancier of organisatie een bewerkingsovereenkomst bovenschools opgevraagd en afgesloten worden. Dit geldt dus ook voor alle (gratis) beschikbare educatieve software en apps.
e. Alle bewerkersovereenkomsten worden bovenschools beoordeeld op inhoud door de Ffunctionaris Ggegevensbescherming en getekend door de bestuurder. Scholen tekenen zelf geen overeenkomsten maar sturen deze bij ontvangst door naar de Ffunctionaris Ggegevensbescherming.
f. Als er geen mogelijkheden zijn om met een aanbieder een bewerkersovereenkomst te sluiten, mogen er als basisregel geen privacy-gevoelige gegevens in het betreffende systeem worden ingevoerd. Als het systeem dit afdwingt of eist kan het alleen gebruikt worden met geanonimiseerde gegevens of als er na nader onderzoek (bovenschools) is vastgesteld dat betreffende partij aan de voorwaarden van het convenant digitale onderwijsmiddelen en Privacy voldoet. Dit laatste is bv ook van toepassing op de omgevingen van Google, Microsoft en Apple omdat met deze partijen geen ~~een~~1-op-1 ~~een~~ overeenkomsten kunnen worden afgesloten.
g. Bij alle overeenkomsten is het geldende convenant "Digitale Onderwijsmiddelen en Privacy" met de bijbehorende modelovereenkomst van o.a. de PO-raad het uitgangspunt.
h. Een getekend~~,~~ exemplaar van iedere bewerkingsovereenkomst wordt bovenschools bewaard.

3.8 Rechten van de betrokkenen

a. Het bevoegd gezag informeert de medewerkers en andere gebruikers voorafgaand aan de invoering van voor hen geldende afspraken zoals in dit handboek opgenomen.
b. Medewerkers of andere gebruikers die problemen ervaren met betrekking tot de naleving van de afspraken rond IBP kunnen dit melden bij de directeur of de Ffunctionaris Ggegevensbescherming. Daarnaast kan ook gebruik gemaakt worden van de geldende klachtenregeling en kunnen ze zich daarbij wenden tot de vertrouwenspersonen.

4. Slotbepaling:

De dagelijkse digitale praktijk verandert voortdurend en in een alsmaar hoger tempo. We zullen dan ook dit handboek als daar aanleiding voor is aanpassen, uitbreiden en bijstellen. Bij elke nieuwe versie zullen we de gebruikers waarop dit handboek betrekking heeft op de hoogte stellen van de aanpassingen.