Privacy beleid SBO De Korenburg
(inclusief privacyverklaring en privacy protocol)

Algemeen

Privacy beleid	: stichting De Korenburg
Ingangsdatum	: 17 mei 2018
Opgesteld door	: Susan Teerink
Vastgesteld op:	: 17-05-2018
Ondertekening:	S.v.Teerink

Organisatie

Dit privacy beleid heeft betrekking op de bescherming van persoonsgegevens van alle betrokkenen van stichting De Korenburg. Het gaat in ieder geval om alle medewerkers, de leerlingen, hun ouders en/of verzorgers en externe relaties. In dit beleid is de privacy verklaring en het privacy protocol opgenomen.
Om ervoor te zorgen dat stichting De Korenburg kan voldoen aan relevante wet- en regelgeving, is het belangrijk dat alle medewerkers op de hoogte zijn van het privacy beleid. Het privacy beleid helpt, met de juiste acties, veilig met persoonsgegevens om te gaan. Door het weergegeven van taken, bevoegdheden en verantwoordelijkheden is het voor een ieder duidelijk wat zijn of haar taak is binnen stichting De Korenburg. Uiteindelijk is elke medewerker verantwoordelijk voor een juiste omgang met persoonsgegevens.

Het doel van dit privacybeleid is om kwaliteit van de gegevensverwerking te optimaliseren waarbij we zoeken naar een goede balans tussen privacy, funktionaliteit en veiligheid. Het uitgangspunt is dat de privacy van de betrokkenen wordt gerespecteerd. De gegevensverwerking moet voldoen aan relevante wet- en regelgeving.

Het privacybeleid beschrijft op strategisch niveau de doelstellingen op het gebied van de bescherming van persoonsgegevens. Het geeft op die manier richting aan de gehele organisatie als het gaat om de verwerking van persoonsgegevens.

Uitgangspunten

Stichting De Korenburg vindt het belangrijk om transparant te handelen, vooral in het kader van de verwerking van persoonsgegevens. Daarom gaat stichting De Korenburg veilig en integer met de persoonsgegevens om en is compliant met de wet- en regelgeving op het gebied van de bescherming van de persoonsgegevens. Bij de werkzaamheden op De Korenburg worden de algemene beginselen op het gebied van de verwerking van persoonsgegevens in acht genomen. Daarnaast worden alle medewerkers getraind op het gebied van privacy om ervoor te zorgen dat de bescherming van persoonsgegevens verzekerd kan worden. Ook zorgt stichting De Korenburg ervoor dat bij het ontwerpen van nieuw beleid, het inrichten van nieuwe processen of andere relevante zaken de begrippen privacy bij design* en privacy bij default** een rol speelt.

Stichting De Korenburg beperkt het verwerken van persoonsgegevens tot de uitdrukkelijke omschreven doelen waarvoor ze verzameld zijn. Daarbij wordt het vereiste van doelbindig nageleefd.
Voor het behandelen van de rechten van de betrokkenen is een procedure ingericht. Op deze manier kan stichting De Korenburg ervoor zorgen dat de betrokkenen hun rechten kunnen uitoefenen.

De inventarisatie en de actualisatie van het verwerkinsregister vindt periodiek plaats (minimaal 1x per half jaar) en indien nodig wordt een privacy impact assessment (PIA) gedaan.

Taken en bevoegdheden binnen de organisatie

Stichting De Korenburg heeft ervoor gekozen om (samen met de Onderwijs Coöperatie Gelderland (OCG) een gezamenlijke) functionaris gegevensbescherming (FG) aan te stellen met als taak toezicht te houden op de naleving van de wet- en regelgeving op het gebied van de bescherming van persoonsgegevens, evenals toezicht op de uitvoering van dit privacybeleid.

Alle medewerkers zijn verplicht om medewerking te verlenen aan de FG indien dit gevraagd wordt. Met name het verwerken van leerlinggegevens speelt op De Korenburg een rol. De personeels- en adminstratie administratie is ondergebracht bij de Cabo. Met dit administratiekantoor heeft stichting de Korenburg een verwerkersovereenkomst.

Algemende beginselen van de bescherming van persoonsgegevens

De verwerking moet voldoen aan de algemene beginselen van de bescherming van persoonsgegevens. De verwerking van persoonsgegevens moet aan de volgende eisen voldoen:

- Verwerkingen moeten rechtmatig, eerlijk en transparant zijn ten opzichte van de betokkenen.
- Persoonsgegevens moeten voor welbepaalde, uitdrukkelijke omschreven en rechtvaardigde doeleinden worden verzameld.

- Persoonsgegevens mogen niet verder worden verwerkt op een met die doeleinden onverenigbare wijze. Verenigbaar met het oorspronkelijke doel zijn verwerkingen voor archivering, doeleinden van algemeen belang, wetenschappelijke en historische onderzoeksdoeleinden en statistische doeleinden.
- Persoonsgegevens moeten adequaat en ter zake dienend zijn en beperkt blijven tot datgene wat minimaal nodig is voor de doeleinden waarvoor zij worden verwerkt.
- Persoonsgegevens moeten accuraat en waar nodig up-to-date- zijn.
- Persoonsgegevens mogen niet langer worden bewaard in een vorm die het mogelijk maat de betrokken te identificeren dan voor verwezenlijking van de doeleinden waarvoor ze worden verwerkt, noodzakelijk is. Persoonsgegevens mogen langer worden bewaard voor archivering in algemeen belang en voor historisch, statistische of wetenschappelijke doeleinden.
- Persoonsgegvens mogen alleen worden verwerkt op een manier die de veiligheid van de persoonsgegevens verzekert. Wanneer verwerking plaatsvindt op grond van gerechtvaardigd belang, één van de 6 wettelijke grondslagen, pas na expliciete afweging van de gevolgen van de verwerking voor de belangen van de betrokkenen en de belangen van de organisatie.

Het is belangrijk dat stichting De Korenburg kan aantonen dat aan deze beginselen wordt voldaan. Eén van de manieren om dit aan te tonen is door het vormgeven, inplementeren en onderhouden van dit privacybeleid.
Daarnaast is de privacyverklaring- onder andere te vinden op de website van stichting De Korenburg- een manier om te voldoen aan de beginselen. Veder worden de werknemers getraind op privacy bewustzijn en zijn processen ingericht om te voldoen aan de beginselen.

Verwerkers

In het geval van verwerking door externe parijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt stichting De Korenburg afspraken over de eisen waar de verwerking aan moet voldoen. Deze afspraken voldoen aan de wet. Stichting De Korenburg controleert deze afpraken minimaal (minimaal 1x per jaar). Bij het aanstellen van een verwerker wordt een verwerkingsovereenkomst gesloten.

Informatiebeveiliging en datalekken

Als uitgangspunt dienen persoonsgegevens beveiligd te worden met passende technische en organisatirische maatregelen. Het beleid voor informatiebeveiliging is apart beschreven (LINK)

Afsluiting

Stichting De Koreburg evalueert het privacybeleid jaarlijks en legt bevindingen vast. Waar nodig vindt een bijstelling van het beleid vast.

*

Privacy by design

Privacy by design houdt in dat u als organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) ten eerste aandacht besteedt aan privacyverhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Ten tweede houdt u rekening met dataminimalisatie: u verwerkt zo min mogelijk persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking. Op deze manier kunt u een zorgvuldige en verantwoorde omgang met persoonsgegevens technisch afdwingen.

**

Privacy by default kan je zien als onderdeel van privacy by design. Het vereist dat de standaardinstellingen altijd zo privacy-vriendelijk mogelijk zien.
Je moet er voor zorgen dat persoonsgegevens niet standaard openbaar te zien zijn. Een profiel op social media is daar een mooi voorbeeld van. Dit mag wel openbaar zijn, maar alleen als een gebruiker daar eerst zelf actief voor kiest. De social media-toepassing zal in de standaardinstellingen de gebruikersprofielen zoveel mogelijk moeten afschermen. Dat principe van afschermen geldt ook voor ICT-toepassingen. Daarbij kun je denken aan browser-instellingen tot bedrijfssoftware. Alles moet ontwikkelt worden met standaardinstellingen die privacy-vriendelijk is.

Privacyverklaring

Stichting SBO De Korenburg
Morsestraat 21a
7101JA Winterswijk
Tel: 0543-512214
info@dekorenburg.nl

Inleiding

Op De Korenburg wordt bewust en zorgvuldig omgegaan met de privacy van onze leerlingen. In verband met het geven van onderwijs, het ondersteunen van onze leerlingen, en de vastlegging daarvan in de administratie van de school, worden er gegevens over en van leerlingen vastgelegd. Deze gegevens worden persoonsgegevens genoemd. Het vastleggen en gebruik van deze persoonsgegevens is beperkt tot informatie die strikt noodzakelijk is voor het onderwijs. De gegevens worden beveiligd opgeslagen en de toegang daartoe is beperkt. De school maakt ook gebruik van digitaal leermateriaal.
De leveranciers van die leermaterialen ontvangen een beperkt aantal leerlinggegevens.
De school heeft haar leveranciers strikte afspraken gemaakt over het gebruik van persoonsgegevens, zodat misbruik wordt voorkomen. Leerlinginformatie wordt alleen gedeeld met andere organisaties als ouders daar toestemming voor geven, tenzij die uitwisseling verplicht is volgens de wet.

Wat zijn persoonsgegevens

Wanneer u uw kind aanmeldt op De Korenburg, vragen wij u om enkele persoonsgegevens te geven. Deze gegevens slaan we op in ons Leerlingvolgsysteem (Parnassys) . U kunt daarbij denken aan uw naam, uw adres, de naam van uw kind(eren). Wij verstrekken deze gegevens niet aan derden zonder uw toestemming tenzij wij daartoe verplicht zijn gezien onze wettelijke taak. Bijvoorbeeld bij een leerplichtmelding en naar de uitvoeringsorganisatie van het Ministerie van Onderwijs (DUO).

Ben u verplicht om persoonsgegevens te verstrekken?

Indien u uw kind aanmeldt op De Korenburg, bent u verplicht om enkele gegevens te verstrekken over uw kind en de verantwoordelijke verzorgers/ouders. Wij beschouwen deze informatie als vertrouwelijke informatie.

Gegevens verzameld bij anderen?

Wij verwerken geen gegevens die we opvragen bij andere instellingen.

Wie is de verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens?

De juridisch verantwoordelijke voor het verwerken van de persoonsgegevens is de directeur bestuurder.

Wie is de functionaris van gegevensbescherming?

De directeur bestuurder is verantwoordelijk voor het beschermen van de egevensverwerking.

Welke persoonsgegevens gebruiken wij?

Wij registreren uw naam, de naam van uw kind(eren), uw adres en telefoonnummer, de geboortedatum en geboorteplaats van de kinderen die bij ons zijn ingeschreven. Wij registreren geen gegevens over medische situaties, geloof of anderszins. Wij registeren informatie over allergieën en medicijnen indien dat noodzakelijk is. We vragen uw toestemming voor het gebruik van uw mailadres voor het sturen van informatie. We delen uw mailadres niet met derden.
Wij dragen er zorg voor dat de persoonlijke informatie die u met uw bezoek aan onze website verschaft, vertrouwelijk wordt behandeld. Persoonsgegevens welke in onze website worden opgegeven worden niet verkocht aan derden. Ook gebruiken we geen social media plugin's. Stichting De Korenburg gebruikt alleen technische en functionele cookies die zorgen voor een goede werking van de websites.
U kunt zich afmelden voor cookies door uw internetbrowser zo in te stellen dat deze geen cookies meer opslaat. Daarnaast kunt u ook alle informatie die eerder is opgeslagen via de instellingen van uw browser verwijderen.

Voor welke doelen gebruiken we uw gegevens?

Wij gebruiken de gegevens over onze leerlingen ten hoeve van de uitvoering van het onderwijs en ook om met u in contact te treden met informatie over uw kind(eren).

Bestaan van geautomatiseerde individuele besluitvorming

Onze stichting maakt geen gebruik van geautomatiseerde verwerkingen die gevolgen kunnen hebben voor personen.

Delen we de gegevens met andere partijen?
We delen de gegevens over uw kind wanneer wij daartoe wettelijk verplicht zijn, met andere overheidsorganisaties. U kunt hierbij denken aan instanties die verantwoordelijk zijn voor de uitvoering van wettelijke taken op het gebied van wettelijke taken op het gebied van jeugd zoals leerplicht.

Wij delen de NAW informatie over uw kind met de dienstverlener die de geautomatiseerde leerlingenadministratie verzorgt. Met deze dienstverlener is een verwerkingsovereenkomst opgesteld.

Worden uw gegevens buiten de EU gebracht?

Uw gegevens worden niet buiten de EU gebracht.

Hoe beveiligen we uw gegevens?

Stichting De Korenburg neemt de bescherming van uw gegevens serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging, tegen te gaan. Heeft u de indruk dat uw gegevens niet goed beveiligd zijn of er zijn aanwijzingen voor misbruik, neem dan contact met ons op via info@dekorenburg.nl

Hoe lang bewaren we uw gegevens?

We bewaren uw gegevens maximaal twee jaar nadat uw kind bij ons van school is gegaan.

Welke rechten hebt u op basis van de verwerking van persoonsgegevens?

U heeft het recht om uw persoonsgegevens in te zien, te corrigeren en te verwijderen. Daarnaast heeft u het recht om uw eventuele toestemming voor gegevensverwerking in te trekken of bezwaar te maken. U heeft ook het recht op gegevensoverdraagbaarheid. Dat betekent dat u bij ons een verzoek kunt indienen om de persoonsgegevens die wij van u registreren, door te sturen naar een andere organisatie. U kunt uw verzoek tot inzage, correctie, verwijdering, beperking, doorsturen of bezwaar, richten aan info@dekorenburg.nl Om er zeker van te zijn dat het verzoek om inzage door u is gedaan, vragen wij altijd een kopie van het identiteitsbewijs mee te sturen. Wij doen dit ter bescherming van uw privacy. We reageren zo snel mogelijk maar in ieder geval binnen vier weken op uw verzoek. U kunt ook een klacht indienen bij de Autoriteit Persoonsgegevens.
Dat kan via de link https://autoriteitpersoonsgegevens.nl/nl/contact

Hoe kunt u contact met ons opnemen?

U kunt contact opnemen met de verantwoordelijke functionaris via het emailadres info@dekorenburg.nl

Privacy protocol

Stichting SBO De Korenburg
Morsestraat 21a
7101JA Winterswijk
Tel: 0543-512214
info@dekorenburg.nl

Protocol en instructies omgaan met privacy gevoelige informatie

Toegang
Fysieke toegang tot werkplekken

De meeste ruimtes op De Korenburg zijn nog niet af te sluiten. Op de administratie komen kasten die op slot kunnen. Het kantoor van de directeur moet met beide deuren af te sluiten zijn, in de deuren worden sloten gemaakt.

Sluit pc's altijd af bij vertrek - ook bij tijdelijk vertrek: stel de schermbeveiliging in bij vertrek uit de ruimte of wanneer het apparaat onbeheerd achter wordt gelaten. (vlaggetje l)

Houdt toegang tot de kantoren en werkplekken strikt voor medewerkers en vrijwilligers die daar daadwerkelijk iets te zoeken hebben

Voorkom dat bezoekers of willekeurige vrijwilligers vrij in en uit kunnen lopen zonder begeleiding.

Digitale toegang tot netwerk

De toegang tot het netwerk is beveiligd met inlogcodes, deze codes zijn persoonlijk en mogen nimmer aan anderen worden vrij gegeven.

Houdt de wificode van de beveiligde wifi omgeving voor personeel geheim- geef deze niet aan bezoekers, vrijwilligers. Publiceer deze code NOOIT op een algemeen toegankelijke ruimte of prikbord.

Bewaren van gegevens

Berg privacygevoelige informatie altijd veilig op:

- **Papieren versie:**
- Niet op een bureau laten slingeren, maar in een afsluitbare kast of lade opbergen. Bij vetrek bureau op slot, kast op slot.
- Sleutel opbergen in sleutelkastje. Dit kastje wordt vervangen door een sleutelkastje met code. Directeur en administratie zullen dit sleutelkastje beheren en kennen de code.
- **Digitale versie:**
- Documenten alleen opslaan op het netwerk – dus bij ingelogd zijn in een beveiligde omgeving- in de daarvoor bestemde mappen.
- Opslaan van documenten op een andere werkschijf van de desktop is niet toegestaan.
- Gebruik van USB stick om privacy gevoelige informatie over te brengen is niet toegestaan.

Bewaartermijn, vernietingen van gegevens

Bewaartermijnen van privacygevoelige informatie die binnen Stichting De Korenburg gehanteerd worden intern:

- de arbeidsovereenkomst	2 jaar na beëindiging
- loonbelastingverklaring	5 jaar
- kopie identiteitsbewijs medewerker	5 jaar
- de klachten behanddeling	niet langer dan twee jaar na de laatste klacht.
- Het funktioneringsgesprek/beoordelings-gesprek	3 jaar

Wanneer rechtspositionele aspecten in het geding zijn, kunnen gegevens uit het personeelsdossier naar buiten gebracht worden. De beoordeling daartoe berust bij de directeur.

Vernietigen van privacy-gevoelige informatie op papier

Voor het vernietigen van enkele stuks privacygevoelige informatie wordt de papier-versnipperaar gebruikt. Grotere hoeveelheden privacy gevoelige stukken worden verzameld in de daarvoor aangewezen dozen en worden afgesloten bewaard. Deze worden vervolgens afgevoerd naar daartoe gespecialiseerde bedrijven die de inhoud vernietigen en daarvoor een verklaring afgeven.

Vernietigen van privacygevoelige digitale informatie

Digitale informatie wordt verwijderd door de ducumenten naar de virtuele prullenmand te verplaatsen en deze prullenmand en deze automatisch (dagelijks bij het afsluiten) te laten legen.
Bij PC's of andere hardware die weggegooid moet worden, deze worden ingeleverd bij de IT-medewerker, die de instellingen en bestanden verwijdert en de apparatuur vervolgens aanbiedt aan een professioneel bedrijf wat de schijven vernietigd, alvorens de hardware in de container belandt. Dit bedrijf geeft daarvoor een verklaring van vernietiging af.

ICT apparatuur en software

Beschikbaarstelling apparatuur

Vanuit de organisatie wordt computerapparatuur beschikbaar gesteld aan die medewerkers voor de uitoefening van hun functie en uitvoering van hun werkzaamheden.
Dit gebeurd aan de hand van een overzicht

Dit overzicht is in beheer bij de gevensbeheerder.
De apparatuur is bedoeld voor zakelijk gebruik. Bij prive gelden de zakelijke richtlijnen m.b.t. beveiliging en veilig gebruik

Bij indiensttreding, functiewisseling of besluit tot toekenning van apperatuur wordt door de medewerker ICT de apperatuur gereed gemaakt voor gebruik en uitgereikt aan de medewerker t.w.:

- Een account aangemaakt en ingesteld, met login en wachtwoord- deze wordt aangevraagd bij de ICT medewerker.
- De apperatuur wordt aan de hand van de aangeleverde informatie over bevoegdheden ingeregeld, waaronder toegang tot het netwerk, toegang tot de veiligde wifi-nettwerken, toegang tot de mappen en netwerkschijven
- De juiste werking van de apparatuur en applicaties wordt uitgecheckt voor uitreiking
- Bij het uitreiken van de apparatuur wordt uitleg gegeven over gebruik en regels over veilig datagebruik
- De medewerker tekent voor ontvangst van de apparatuur en het bekend zijn met de richtlijnen voor dataveilig gebruik.

De ICT medewerker is (dagelijks) contactpersoon in de organisatie voor vragen over ICT en onderhoudt de contacten m.b.t. beheer, service en onderhoud van de systemen met de ICT partners. De ICT medewerker beheert de uitgifte en inname van de ICT apparatuur en houdt daarvan registratie bij.

Omgaan met dataverkeer en ICT apparatuur

- Iedere medewerker die een pc, laptop of tablet ter beschikking heeft krijgt, krijgt daarbij instructie over hoe om te gaan met veilig werken.
- Deze apparatuur wordt vooraf ingesteld op de voor de medewerker toegankelijke programma's, documenten en mappen.
- Software, indien afwijkend van de standaard software, wprdt pas na akkoord door de leidinggevende en na beoordeling op veilig gebruik, door de ICT medewerker, op een

device geinstalleerd of vrijgegeven. Medewerkers mogen niet zelf software installeren op de hardware die de organisatie ter beschikking stelt.

- Alle ICT apparatuur, ook de persoonlijke die zakelijk gebruikt worden, moeten zijn beveiligd met een goed wachtwoord (minimaal 9 cijfers/tekens)
- Voor elke medewerker wordt toegang tot het netwerk gerealiseerd.
- De medewerker ontvangt een inlogcode en wachtwoord. Bij eerste keer inloggen door de medewerker dient het standaard wachtwoord meteen gewijzigd te worden. Er geldt een wachtwoordbeleid waaraan ieder zich te houden heeft.
- Toegang tot het vaste netwerk binnen de kantoren van stichting De Korenburg vindt plaats door de inlognaam en wachtwoord.
- Toegang tot het netwerk via wifi verbinding op andere locaties vindt plaats door inloggen met inlognaam, wachtwoord (optioneel: waarna een tweede authenticatie via sms plaats
- Voor medewerkers die toegang moeten hebben tot de wifinetwerken wordt de toegang specifiek voor die netwerken ingesteld op het zakelijke device.
- Het automatisch zoeken naar 'bekende netwerken' op laptop, tablet of smartphone moet uit staan.
- Wanneer een dataverbinding nodig is in geval bij bezoek aan een client, moet de (eigen) mobiele telefoon gebruikt worden als hotspot en voor de dataverbinding. Of wordt gebruik gemaakt van de door de organisatie afgesloten VPN verbinding.
- Het gebruik van het wifinetwerk van een client is niet toegestaan.
- Het gebruik van onbeveiligde internetverbindingen (vrije wifinetwerken, zonder inlogcode) is niet toegestaan.
- Sla geen persoonsgegevens op op draagbare apparaten en sticks (usb, tablets, mobiele telefoons, laptops) maar gebruik daarvoor het beveiligde netwerk.
- Print altijd met uitgestelde printfunctionaliteit en de daarbij behorende code, zodat prints met persoonsgegevens niet onbeheerd bij de printer liggen.
- Print zo min mogelijk gegevens af en houd die gegevens zo veel mogelijk binnenshuis.
- Verstuur zo min mogelijk persoonsgegevens per mail en nooit zonder toestemming van de persoon waarover het gaat.
- Mail bij voorkeur vanuit de kantoor- of klassenomgeving of via een secure-mail oplossing via de VPN berbinding.
- Geprinte documenten met persoonsgegevens die weggegooid worden moeten altijd door een papiervernietiger gehaald worden, danwel in een daarvoor bestemde papierbak in een afgesloten ruimte gedaan worden.

Het wachtwoordbeleid bij stichting De Korenburg is als volgt:

Wachtwoorden mogen niet worden opgeslagen in het netwerk

De enige uitzondering is om een wachtwoordmanager zoals Keepass aap te gebruiken die op het bureaublad is geïnstalleerd waarin wachtwoorden kunnen worden opgeslagen. Ook deze is met een wachtwoord beveiligd, mar dan hoeft er slechts 1 wachtwoord onthouden te worden.
Wachtwoorden opslaan in een notitieboekje, op post-its etc is niet toegestaan/.

Netwerk en applicaties

Samenstelling wachtwoord voor inloggen op het netwerk:

Minimaal 9 tekens
dat moet zijn een combinatie van cijfers, kleine letters en hoofdletters en tekens.
Periode van wijzigen 1x per drie maanden

Voorwaarde nieuwe wachtwoorden:

- Wachtwoorden mogen de eerstvolgende 6 keer niet opnieuw gebruikt worden.
- Wachtwoorden mogen niet opvolgend zijn

Samenstelling wachtwoord voor inloggen op het specifieke applicaties, zoals **leerlingvolgsysteem:**