PROO LEIDEN LEIDERDORP

Stichting Openbaar Primair en Speciaal Onderwijs Leiden-Leiderdorp

Beleidsplan Privacy

PROOLeiden - Leiderdorp

Versie 2.1| december 2019

ONDERWIJS MET AANDACHT VOOR ELKAAR

Elisabethhof 17 • 2353 EW Leiderdorp • 071 524 76 70
mail@prooleiden.nl • www.prooleiden.nl

5.1.1 Bron

Kennisnet

5.1.2 Bewerkt door:

PROOLeiden, OBSG Leiderdorp

Versie	Status	Datum	Auteur	Omschrijving
1.0	concept	Februari 2019	M. van Velsen	Besproken met: BT februari 2018 BOD 8 maart 2018
2.0	concept	Nov 2019	M. van Velsen	Besproken met: FG 05/11/19 BT 11/11/19 BOD 14/11/19 AVG klanbordgroep 25/11/2019
2.1	concept	Nov 2019	M. van Velsen	Aanpassingen nav bovenstaande besprekingen

5.1.3 Vastgesteld door

Versie	Datum	Naam	Functie
Def	8/4/20	M. de Pinth	Directeur-bestuurder

1. Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ict. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ict.

Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ict en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee.

Het goed regelen van **informatiebeveiliging en privacy** (IBP) in een privacybeleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen. Dit document beschrijft de kaders hiervoor.

2. Toelichting Informatiebeveiliging en Privacy

2.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.

Informatiebeveiliging richt zich op de volgende aspecten:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imagoverlies.

2.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt o.a. onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of

indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan.

De wet noemt als voorbeelden van verwerking:
Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

2.3 Vervlechting informatiebeveiliging en privacy

Informatiebeveiliging is een belangrijke voorwaarde voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk.

Het Privacy Beleidsplan vormt de basis om informatiebeveiliging en privacy binnen PROOLeiden-Leiderdorp te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3. Doel en reikwijdte

3.1 Doel

Informatiebeveiliging en privacy hebben de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan PROOLeiden-Leiderdorp persoonsgegevens verwerkt, waaronder leerlingen, ouders/verzorgers en medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het privacybeleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid.

De persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en ouders/verzorgers) wordt gerespecteerd en PROOLeiden-Leiderdorp voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

Het privacybeleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen PROOLeiden-Leiderdorp waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan PROOLeiden-Leiderdorp persoonsgegevens verwerkt. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.

Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van PROOLeiden-Leiderdorp. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (bijvoorbeeld uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en/of sociale media.)

Het privacybeleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van PROOLeiden-Leiderdorp evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen.

Het privacybeleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Privacybeleid heeft binnen PROOLeiden-Leiderdorp raakvlakken met:

- *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen;
- *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties;
- *ICT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen;
- *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers.

4. Uitgangpunten beleid

PROOLeiden-Leiderdorp hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

- Het schoolbestuur van PROOLeiden-Leiderdorp neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.

- PROOLeiden-Leiderdorp voldoet aan alle relevante wet- en regelgeving.

- Bij PROOLeiden-Leiderdorp is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen.

- Een goede balans tussen het belang van PROOLeiden-Leiderdorp om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen te allen tijde hun toestemming herzien.

- PROOLeiden-Leiderdorp zal alle betrokkenen helder en actief informeren over de verwerkingen van hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.

- PROOLeiden-Leiderdorp legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. PROOLeiden-Leiderdorp voldoet hiermee aan de documentatieplicht.

- Binnen PROOLeiden-Leiderdorp 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 die van papieren documenten.

- PROOLeiden-Leiderdorp is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

- PROOLeiden-Leiderdorp classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen

maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.

- PROOLeiden-Leiderdorp sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.

- PROOLeiden-Leiderdorp verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties 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. PROOLeiden-Leiderdorp heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

- Informatiebeveiliging en privacy is bij PROOLeiden-Leiderdorp een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

- PROOLeiden-Leiderdorp kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

- PROOLeiden-Leiderdorp neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.

- Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt PROOLeiden-Leiderdorp aanvullende afspraken vast over de technische maatregelen.

- PROOLeiden-Leiderdorp zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen

5. Uitwerking van het beleid

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid. Gedetailleerde uitwerking van de beleidspunten en kaders zijn terug te vinden op Sharepoint, Teams of op het AVG Portal.

5.2 Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur PO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

5.3 Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens te weten:

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 verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.

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 (subsidiair). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Transparantie**: de school legt aan betrokkenen (leerlingen, ouders/verzorgers en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde privacybeleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.

5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

5.4 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. De AVG Portal/sharepoint/Teams geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

5.5 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt 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 de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten.

Verhoging van het bewustzijn omtrent privacy is een gezamenlijke verantwoordelijkheid van de bestuurssecretaris, teamleider ICT en de FG, met het bestuur als eindverantwoordelijke. Zij worden hierin ondersteund door het thema team Communicatie. In het thema team wordt gesproken over communicatie en het creëren van bewustzijn in de organisatie m.b.t. Informatiebeveiliging en Privacy.

5.6 Classificatie en risicoanalyse

Alle informatie heeft waarde. Daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de betrouwbaarheidsaspecten die van belang zijn.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe

(informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ict)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

5.7 Incidenten en datalekken

Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld bij **meldpuntdatalekken@prooleiden.nl**

Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.8 Planning en controle

Dit privacybeleid wordt minimaal elk jaar getoetst en bijgesteld door het bestuur. Hierbij wordt rekening gehouden met:

- de status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
- de actuele geinventariseerde risico's;
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan.

Daarnaast kent PROOLeiden-Leiderdorp een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces, samen met de FG, waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst (oa met een hiervoor onwikkelde scan). Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

5.9 Naleving en sancties

Naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op het al dan niet uitvoeren van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan privacy bij de aanstelling, tijdens functioneringsgesprekken, met een instellingsbrede gedragscode, met periodieke bewustwordingscampagnes etc.

Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. Daarnaast adviseert de FG over te nemen maatregelen. De FG wordt aangesteld door het bestuur en heeft een

wettelijk omschreven en onafhankelijke toezichthoudende taak (artikel 37-38 AVG).

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan PROOLeiden-Leiderdorp de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.10 Logging en monitoring

Logging en monitoring zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Zie hiervoor de zogenaamde autorisatiematrix. Hieronder vallen o.a. het in- uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

6. Organisatie

6.1 Rollen en verantwoordelijkheden

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij PROOLeiden-Leiderdorp een aantal taken en verantwoordelijkheden onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

Beschreven wordt welke rollen, welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Directeur-bestuurder

De directeur-bestuurder is als bevoegd gezag van de stichting eindverantwoordelijk en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.

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

De inhoudelijke verantwoordelijkheid voor het privacybeleid is gemandateerd aan de bestuurssecretaris en teamleider ICT.

Bestuurssecretaris

De bestuurssecretaris geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau.

De bestuurssecretaris moet:

- het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- de uniformiteit bewaken binnen PROOLeiden-Leiderdorp
- het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- de verdere afhandeling van incidenten binnen PROOLeiden-Leiderdorp coördineren.

De bestuurssecretaris werkt hierbij nauw samen met teamleider ICT en de FG.

Teamleider ICT

De teamleider ICT adviseert samen met de bestuurssecretaris de directeur-bestuurder en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen PROOLeiden-Leiderdorp. De teamleider ICT faciliteert en coördineert de ICT-coördinatoren met hun werkzaamheden m.b.t. informatiebeveiliging en privacy.

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) houdt binnen PROOLeiden-Leiderdorp toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het verbeteren en stimuleren van bewustwording rondom privacy, het afhandelen van informatiebeveiligingsincidenten, adviseert over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (het bestuur). De FG heeft regelmatig overleg met de bestuurssecretaris en de teamleider ICT. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

Leidinggevenden algemeen

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

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

Schoolleiders

Op de schoollocaties ziet de schoolleider erop toe dat het privacybeleid wordt geïmplementeerd en nageleefd. Zij zijn ervoor verantwoordelijk dat medewerkers in de scholen zich gedragen conform afspraken. De schoolleiders hebben hierbij een voorbeeldrol ten opzichte van de medewerkers.

Op ieder school krijgt een medewerker de rol van privacy-medewerker. Deze medewerkers is, naast de schoolleider, aanspreekpunt voor medewerkers.

Teamleiders bestuursbureau

Binnen de organisatie zijn er bovenschools georganiseerde processen zoals ict, personeel (HRM, P&O), administratie, facilitaire en financiële zaken et cetera. Voor elk van deze processen is een teamleider verantwoordelijk om te bepalen op welke wijze privacy daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies. De teamleiders hebben een rol in het opstellen en bijhouden van de verwerkingen van persoonsgegevens in het verwerkingsregister, de verwerkingsovereenkomsten e.d.

Deze teamleider is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen ten onrechte toegang krijgen tot applicaties.

Om deze risico's te verkleinen hebben de teamleiders de volgende specifieke taken:

- Samen met de directeur-bestuurder stellen zij het beleid voor toegang (autorisaties) vast.
- Samen met ICT-beheer zien zij erop toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn o.a. beschreven in functieprofielen. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met trainingen, checklists en formulieren.

Medewerkers wordt gevraagd om actief betrokken te zijn bij informatiebeveiliging en privacy. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR).

Privacyteam

Het privacy team van PROOLeiden-Leiderdorp heeft de volgende opdracht:

- het geven van voorlichting en het doen van algemene aanbevelingen.
- het ondersteunen bij ontwikkeling, implementatie en borging van het privacybeleid.

ICT-coördinatoren

De ICT-coördinatoren spelen een belangrijke rol in het vergroten van het bewustzijn rondom privacy op de scholen. Zij zijn vraagbaak voor medewerkers.

7. Documentatie

SharePoint/teams/intranetsite bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen, als uitwerking van de kaders uit dit document.

Overzicht:

- Jaarplanning IBP
- Autorisatiematrix
- Procedure toestemming gebruik beeldmateriaal
- Toestemmingsbrief
- Procedure opschonen van gegevens
- Rechten betrokkenen
- Procesbeschrijving Rechten betrokkenen
- Privacyreglement
- Privacyverklaring leerlingen
- Privacyverklaring medewerkers
- Privacy- en cookie verklaring (voor bezoekers website)
- Autorisatiematrix
- AVG-bewustwordingsplanning
- Protocol Cameratoezicht
- Wachtwoordbeleid
- Responsible disclosure
- Gedragscode gebruik e-mail, ICT en sociale media
- Overzicht overlegmomenten FG en privacy vertegenwoordiging
- Procesbeschrijving melden datalekken
- Registratie beveiligingsincidenten
- Verwerkingsregister
- Verwerkersovereenkomsten
- Procedure gegevensbeschermingseffectbeoordeling
- Procedure DPIA - risicoanalyse
- Enquête schoolleiders, medewerkers