Hogeschool der Kunsten Den Haag

University of the Arts The Hague

Koninklijk Conservatorium Royal Conservatoire

Koninklijke Academie van Beeldende Kunsten Royal Academy of Art

Informatiebeveiliging en privacy
Beleid van Hogeschool der Kunsten Den Haag

Bron
Kennisnet, SURF
Beleidsplan Informatiebeveiliging 2016
HdK Beleid Verwerking Persoonsgegevens April 2018
Privacy Reglement Verwerking Persoonsgegevens Mei 2018

Bewerkt door:
Hogeschool der Kunsten Den Haag

Versie	Datum	Omschrijving	Auteur(s)
0.1	24-04-2019	Initiele herziene versie obv Privacy Beleid & Reglement (2018) en Security Beleid (2016).	J. vdBlom
0.2	02-05-2019	Review commentaar verwerkt	W. Harrewijn J. vdBlom
0.3	06-05-2019	Aanpassing IBP-rollen	W. Harrewijn J. vdBlom
0.4	16-05-2019	Review commentaar K. vdLee en G. Coleman verwerkt	J. vdBlom
1.0	22-05-2019	Ter goedkeuring CvB	

Vastgesteld door Hogeschool der Kunsten Den Haag :

Versie	Datum	Naam	Functie
		M. Schoenmakers	**Voorzitter CvB**

Inhoudsopgave

1 Het belang van informatiebeveiliging en privacy ____ *3*

1.1 Informatiebeveiliging ____ 4

1.2 Privacy ____ 4

1.3 Vervlechting informatiebeveiliging en privacy ____ 5

2 Doel en reikwijdte ____ *6*

2.1 Doel ____ 6

2.2 Reikwijdte ____ 6

3 Uitwerking van het beleid ____ *8*

3.1 Relevante wetten en regelgeving ____ 8

3.2 Basisregels bij informatiebeveiliging ____ 8

3.3 Basisregels bij het omgaan met persoonsgegevens ____ 9

3.4 Spelregels IBP ____ 10

4 Ondersteunende richtlijnen en procedures ____ *12*

4.1 Voorlichting en bewustzijn ____ 12

4.2 Rechtmatige verwerking persoonsgegevens ____ 12

4.3 Classificatie en beveiliging ____ 12

4.4 Incidenten en datalekken ____ 12

4.5 Planning en controle ____ 13

4.6 Naleving en sancties ____ 13

4.7 Logging en monitoring ____ 13

5 Organisatie: Wie doet wat? ____ *14*

5.1 Rollen en verantwoordelijkheden ____ 14

Bijlage A: Afkortingen & Definities ____ *17*

Bijlage B: Ondersteunende richtlijnen en procedures ____ *18*

1 Het belang van informatiebeveiliging en privacy

Het hoger 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. Opslag en verwerking van persoonsgegevens dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van persoonsgegevens grote schade kan berokkenen aan studenten, medewerkers en andere betrokkenen.

Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid 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.

Het College van Bestuur van Hogeschool der Kunsten Den Haag (HdK) is wettelijk verantwoordelijk voor het op een juiste manier verwerken van persoonsgegevens.

Met de organisatorische en technische maatregelen beschreven in dit beleidsdocument neemt HdK haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van (persoons-) gegevens te optimaliseren en daarmee te voldoen aan de relevante regel- en privacywetgeving.

Het beleid en bijbehorende reglementen en procedures geven studenten, medewerkers en andere betrokkenen inzicht in hoe privacy en informatiebeveiliging geregeld is op HdK. Daarnaast helpt het bij het creëren van bewustwording over het belang en de noodzaak van het beschermen van persoonsgegevens. Daarnaast is beschreven welke rollen betrokken zijn bij de uitvoer van dit beleid.

Het beleid beoogt:

- Het bieden van een kader: om (toekomstige) verwerkingen van persoonsgegevens te toetsen aan een vastgestelde norm en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie eenduidig te beleggen.
- Het stellen van technische en organisatorische normen. Maatregelen worden genomen op basis van 'best practises' vanuit SURF.
- Het nemen van verantwoordelijkheid door het College van Bestuur: door de uitgangspunten en de organisatie van het verwerken van persoonsgegevens vast te leggen voor de hele HdK.
- Daadkrachtige implementatie van het IBP-beleid door duidelijke keuzes in maatregelen te maken en actieve controle toe te passen op de uitvoering van de beleidsmaatregelen. Dit wordt uitgevoerd door het CvB en het IBP-team.
- Compliant zijn met de Nederlandse en Europese wetgeving.

1.1 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:

- Beschikbaar: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Betrouwbaar: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Beveiligd: 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 schades en imagoverlies.

1.2 Privacy

Privacy gaat over persoonsgegevens en verwerking daarvan. Persoonsgegevens moeten beschermd worden volgens de huidige wetten regelgeving. Bescherming van de privacy regelt onder welke voorwaarden persoonsgegevens verwerkt mogen worden.
HdK heeft in verwerkingsregisters vastgelegd welke persoonsgegevens gebruikt mogen worden voor welk doel. Dit heet ook wel doelbinding en is gekoppeld aan een grondslag. Het doel waar gegevens voor worden gebruikt moet helder zijn omschreven en gecommuniceerd worden aan de betrokken persoon.
De grondslagen zijn:

1. Wettelijke bepaling
2. Contract of overeenkomst
3. Vitaal belang
4. Gerechtvaardigd belang
5. Algemeen Belang
6. Toestemming van betrokkene

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.

Binnen HdK zijn 3 grote groepen, waarvan persoonsgegevens worden vastgelegd, actief: Medewerkers (vast, periodiek, inhuur), Studenten/Scholieren (inclusief ouders) en Gasten. Van deze groepen legt HdK, afhankelijk van de rol of betrekking, persoonsgegevens vast. Deze gegevens (niet limitatief) variëren van NAW-gegevens, VOG-verklaringen, bankgegevens, aanmeldingsdossiers, ID-documenten, IND-dossiers, toets en examenresultaten, studieadviezen, verslaglegging medische controles, afstudeerdossiers, behaalde getuigschriften tot beveiligingscamera beelden.

Een bijzondere groep binnen de AVG-wetgeving is kinderen jonger dan 16 jaar. Voor deze groep zal vaker toestemming gevraagd moeten worden en hebben de standaard risicoklasse Hoog. Voor kinderen onder de 12 jaar geldt dat ouders altijd akkoord moeten geven.

1.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP. Dit beleid vormt de basis op informatiebeveiliging en privacy binnen HdK en vormt de kapstok voor de onderliggende afspraken en procedures.

2 Doel en reikwijdte

2.1 Doel

IBP-beleid heeft de volgende doelen:

1. Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
2. Het garanderen van de privacy van alle betrokkenen waarvan HdK persoonsgegevens verwerkt, waaronder studenten, leerlingen, hun ouders/verzorgers en medewerkers
3. Beveiliging- en privacy incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het IBP-beleid 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. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en studenten) wordt gerespecteerd en HdK voldoet aan relevante wetten regelgeving.

2.2 Reikwijdte

Het IBP-beleid binnen HdK geldt voor alle medewerkers, studenten, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing). Onder dit beleid vallen ook alle apparaten (computers, laptops, mobiele telefoons, etc) van waar geautoriseerde toegang tot het HdK-netwerk verkregen kan worden. Het HdK-netwerk omvat alle technische netwerken (ook wifi) van het Koninklijk Conservatorium en Koninklijke Academie. Dit netwerk wordt onder andere gebruikt voor toegang tot mail, intranet, opslag van bestanden en internet.

Het beleid geldt voor die toepassingen (geautomatiseerde of handmatige verwerking van persoonsgegevens), die vallen onder de verantwoordelijkheid van HdK. Het beleid geldt zowel voor digitale als fysieke gegevensverzamelingen. Hieronder valt tevens de gecontroleerde informatie, die door de hogeschool zelf is gegenereerd en wordt beheerd. De niet-gecontroleerde informatie waarop de hogeschool kan worden aangesproken en kan leiden tot imagoschade valt onder dit beleid middels een gedragscode voor medewerkers en studenten/leerlingen. Een voorbeeld is uitingen op social media.

Het beleid betreft niet het verwerken van persoonsgegevens voor persoonlijk gebruik, zoals persoonlijke werkaantekeningen of een verzameling visitekaartjes.

Beoogd wordt de persoonlijke levenssfeer van de betrokkene zoveel mogelijk te respecteren. De gegevens, die betrekking hebben op een betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik en tegen verlies dan wel misbruik op basis van het fundamenteel recht op bescherming van zijn/haar persoonsgegevens. Dit brengt met zich mee dat het verwerken van persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat persoonsgegevens veilig zijn bij HdK.

IBP-beleid heeft binnen HdK raakvlakken met:

- ***Algemeen veiligheids- en toegangsbeveiligingsbeleid****;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
- ***Personeels-, financieel- en organisatiebeleid****;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
- ***IT-beleid***; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen
- ***Medezeggenschap*** van leerlingen, studenten en medewerkers
- ***Onderwijsbeleid,*** *met als aandachtspunt het gebruik van (persoons-) gegevens binnen en buiten het college en digitalisering van het onderwijs.*
- ***Onderzoeksbeleid,*** *met als aandachtspunt de bescherming van (persoons-) gegevens en resultaten van onderzoek.*

Naast bovenstaande concrete doelstellingen is een meer algemeen doel het creëren van bewustwording van het belang en de noodzaak van het beschermen van Persoonsgegevens, mede ter vermijding van risico's als gevolg van het niet compliant zijn met de relevante wet- en regelgeving.

3 Uitwerking van het beleid

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

3.1 Relevante wetten en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante weten regelgeving, waaronder:

Algemeen

- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Archiefwet
- Auteurswet
- Wetboek van Strafrecht
  o.a. computercriminaliteit III (01-03-2019)

Hogeronderwijs

- Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW)

Primair- en voortgezetonderwijs* (School van Jong Talent)*leeftijdscategorien

- Wet op het primair onderwijs (WPO)
- Wet voortgezet onderwijs (WVO)
- Wet onderwijstoezicht (WOT)
- Leerplichtwet (LPW)

3.2 Basisregels bij informatiebeveiliging

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen. Volgens deze normen behoort informatie te worden geclassificeerd of ingedeeld in risicogroepen. Naast classificatie van gegevens op basis van vertrouwelijkheid is ook classificatie nodig van het belang van de informatie voor het onderwijsproces in termen van beschikbaarheid en integriteit. Deze classificatie heeft behalve op de gegevens ook betrekking op processen, (computer)apparatuur, software, ruimten en personeel. De classificatie levert een score op die bepaald welk niveau van beveiliging vereist is.

De mate van informatiebeveiliging is bepaald op basis van 3 handvatten

1. **Beschikbaar;** informatie moet beschikbaar en toegankelijk zijn. Classificatie gaat in op de mogelijke gevolgen als informatie, of een informatie set, niet beschikbaar is.
2. **Betrouwbaar;** Het in overeenstemming zijn van informatie met de werkelijkheid (informatie is juist, volledig en actueel). Goed beheer van bevoegdheden en mogelijkheden tot muteren, toevoegen, of vernietigen van gegevens voor een gedefinieerde groep gerechtigden is cruciaal voor de integriteit van informatie. Classificatie gaat in op de mogelijke gevolgen wanneer informatie onjuist, onvolledig is of niet actueel is.
3. **Beveiligd**; De bevoegdheden en mogelijkheden om kennis te nemen van informatie voor een gedefinieerde groep gerechtigden. Classificatie gaat in op de mogelijke

gevolgen wanneer informatie in handen komt van derden die hiertoe niet zijn geautoriseerd.

3.3 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.
   - **Wettelijke bepaling**
     Soms bestaat er een wettelijke verplichting op basis waarvan persoonsgegevens wel verwerkt moeten worden. Die verplichtingen staan dan in een andere wet.
   - **Contract of overeenkomst**
     Deze grondslag maakt verwerking van persoonsgegevens mogelijk wanneer dat nodig is voor de uitvoering van de overeenkomst. Het gaat dan uiteraard om een overeenkomst waarbij de betrokkene (de persoon waarvan de persoonsgegevens zijn) partij is.
   - **Vitaal belang**
     Om de vitale belangen van een natuurlijk persoon te kunnen beschermen, mogen de persoonsgegevens verwerkt worden. Maar alleen als de verwerking noodzakelijk is om die vitale belangen te kunnen beschermen
   - **Gerechtvaardigd belang**
     Het gerechtvaardigd belang is eigenlijk vooral een belangenafweging. De verwerking moet noodzakelijk zijn voor de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde, tenzij de privacybelangen van de betrokkene zwaarder wegen. Hierbij moet bijvoorbeeld rekening gehouden worden met de vraag in hoeverre de betrokkene had mogen verwachten dat de verwerking plaats zou vinden en met welk doel dan.
   - **Algemeen Belang**
     Als er een taak van algemeen belang vervuld moet worden waarvoor de verwerking van persoonsgegevens noodzakelijk is, dan mogen de persoonsgegevens verwerkt worden. Dit geldt ook voor taken in het kader van de uitoefening van het openbaar gezag die aan de verwerkersverantwoordelijke zijn opgedragen.
   - **Toestemming van betrokkene**
     Toestemming kan gegeven worden door een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting. De toestemming moet uitdrukkelijk zijn. Stilzwijgende toestemming is niet voldoende
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 staan tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Transparantie**: de hogeschool legt aan betrokkenen (Studenten, leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. 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.

3.4 Spelregels IBP

HdK hanteert de volgende spelregels om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het CvB van HdK neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging- en privacybeleid bekend is, geborgd en uitgevoerd wordt. Het CvB is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.

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

3. HdK 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.

4. Binnen HdK is het veilig en betrouwbaar omgaan (incl delen) met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen, informatiedragers en de daarin opgeslagen informatie, maar ook van papieren documenten.

5. HdK verwacht van alle medewerkers, studenten, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich volgens de gedragscode gedragen met een eigen verantwoordelijkheid en de vastgestelde regels naleven. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. HdK heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

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

7. HdK zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. De proces en applicatie eigenaar zijn hiervoor verantwoordelijk. 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.

8. Bij HdK is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één of meer van de wettelijke grondslagen. Een goede balans tussen het belang van HdK 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.

9. HdK legt alle verwerkingen en bewaartermijnen van persoonsgegevens vast in een dataregister en zal deze dit up-to-date houden. HdK voldoet hiermee aan de documentatieplicht.

10. HdK zal persoonsgegevens (data en documenten) verwijderen of anonimiseren zodra de bewaartermijn is verlopen. Dit geldt ook voor de fysieke archieven of verzamelingen.

11. HdK 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.

12. HdK 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 HdK aanvullende afspraken vast over de technische maatregelen.

13. HdK 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.

14. HdK zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen

4 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage B 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.

4.1 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, studenten, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de Hoofd ICT en Hoofd/Adjunct directeur met het bestuur als eindverantwoordelijke.

4.2 Rechtmatige verwerking persoonsgegevens

Onder AVG mogen niet zomaar persoonsgegevens verwerkt worden. HdK Den Haag moet daarvoor een zogeheten wettelijke grondslag hebben. Daarom is het verplicht om vooraf inzicht te hebben in het type persoonsgegevens dat verwerkt worden en wie binnen of buiten HdK Den Haag deze gegevens kan verwerken. Dit is van toepassing op vele processen en procedures binnen HdK. In bijlage B zijn richtlijnen en procedures aangegeven die hier invulling aan geven.

4.3 Classificatie en beveiliging

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.

4.4 Incidenten en datalekken

Alle medewerkers, studenten en/of leerlingen, die een beveiligingsincident of datalek vermoeden melden dit. 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 FG@HdKdenhaag.nl
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

4.5 Planning en controle

Dit IBP-beleid wordt minimaal elke twee 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 geïnventariseerde risico's;
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent HdK een jaarlijkse kwaliteitstoets als onderdeel van de Plan-Do-Check-Act cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het IBP wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, weten regelgeving et cetera meegenomen.

4.6 Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving 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 IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement.

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

4.7 Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in-/uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

5 Organisatie: Wie doet wat?

5.1 Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij HdK.

Binnen HdK zal het IBP-team het IBP-beleid richting geven en toezien op naleving. In dit team zijn de voornaamste gebruikersgroepen vertegenwoordigd. Het IBP-team komt periodiek bij elkaar. In het overleg valideert het IBP-team de voortgang, naleving, bewustwording en aanvullend te nemen acties. Hiermee dekt het team de cyclus af van Plan – Do – Check – Act (PDCA) voor het IBP-beleid.
Onderwerpen voor dit overleg zijn:

- Datalekken
- Verwerkingsregisters
- Verwerkersovereenkomsten
- Aanpassingen protocollen
- Beveiligings- en privacy impact op nieuwe initiatieven
- Mate van bewustwording personeel en studenten

Het IBP-team zal toezien op het juist gebruik van de verschillende protocollen en registers.

Het IBP-team toets jaarlijkse de kwaliteit van uitvoering en naleving van het informatiebeveiliging- en privacybeleid.
Advies wordt uitgebracht aan CvB en FG.
Het CvB blijft eindverantwoordelijk voor de borging en uitvoering van het IBP-beleid.

Het team bestaat uit de volgende rollen:

- Hoofd ICT/IPO (voorzitter IBP)
- Adjunct-Directeur Bedrijfsvoering KC
- Hoofdbedrijfsvoering KA
- Hoofd P&O
- MarCom (KC & KA)

Op uitnodiging kan het team worden uitgebreid met:

- CvB
- Afdelingshoofden en andere leidinggevenden

Niveau	Functionaris	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	CvB	Eindverantwoordelijk IBP-beleidsvorming, -vastlegging en het uitdragen ervan Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens Evalueren toepassing en werking IBP-beleid op basis van rapportages Organisatie IBP inrichten	IBP beleid Baseline / basismaatregelen Reglement FG vaststellen Privacyreglement vaststellen
Sturend (tactisch)	Hoofd ICT (Focus algemeen en digitaal)	Inhoudelijk verantwoordelijk voor IBP IBP-planning en controle Adviseert bestuur/CvB/directie over IBP Voorbereiden uitvoerend IBP-beleid, Classificatie/risicoanalyse Hanteren IBP-normen en wijze van toetsen Evalueren IBP-beleid en maatregelen Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	Processen, richtlijnen en procedures IBP, waaronder: • Activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Brief toestemming gebruik beeldmateriaal • Opstellen informatie documentatie richting studenten, leerlingen, ouders / verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ICT en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris Gegevensbescherming	Toezicht op naleving privacywetgeving	
	Informatie Protectie Officer (IPO) (Uitgevoerd door Hoofd ICT)	Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens Voorlichting privacy en stimuleren bewustwording	Privacyreglement, Procedure IBP-incident afhandeling Inrichten meldpunt datalekken
	hoofd/adj.dir Bedrijfsvoering Hoofd P&O (focus digitaal & fysiek) MarCom	Voorbereiden uitvoerend IBP-beleid Hanteren IBP-normen en wijze van toetsen Evalueren IBP-beleid en maatregelen Classificatie/risicoanalyse in samenwerking met Hoofd ICT Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door CvB Communicatiestrategie rondom IBP	Inventariseren waar persoonsgegevens van de hogeschool terechtkomen (leveranciers lijst); input dataregister Classificatie- en risicoanalyse documenten. Mate van bewustwording medewerkers en studenten

Uitvoerend (operationeel)	IPO	Incidentafhandeling (registreren en evalueren). Technisch aanspreekpunt voor IBP-incidenten.	
	Dagelijkse leiding/ leidinggevende/ directie/ afdelingshoofden	Communicatie naar alle betrokkenen; • zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan CvB	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken
	Medewerker	Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	

Bijlage A: Afkortingen & Definities

AVG	**Algemene Verordening Gegevensbescherming** (vanaf 2016), is een Europese verordening die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert. De verordening geldt wereldwijd voor alle ondernemingen en organisaties die persoonsgegevens bijhouden en verwerken van natuurlijke personen in de Europese Unie, onafhankelijk of er al dan niet betaald wordt voor diensten of producten. De AVG vervangt de Wbp.
CVB	College van Bestuur
FG	Functionaris Gegevensbescherming. Controleert en adviseert CvB en HdK vanuit de AVG.
HdK	Hogeschool der Kunsten Den Haag.
IBP	Informatiebeveiligingsbeleid en Privacy, beleid voor informatiebeveiliging en privacy.
ICT	Informatie- en Communicatietechnologie
ID	Identiteitskaart, zoals paspoort of rijbewijs
IND	Immigratie- en Naturalisatiedienst. Nederlands overheidsorganisatie
IPO	Informatie Protectie Officer, vervanger voor de FG
ISO	Marktstandaard voor bijvoorbeeld IT-beveiliging, ISO 27001.
LPW	Leerplichtwet, van toepassing bij School Voor Jong Talent.
NAW	Naam, adres, woonplaats. Soms ook als NAWTE met telefoon en email.
NEN	Marktstandaard voor bijvoorbeeld IT-beveiliging, NEN7510 voor zorginstellingen.
OOP	Ondersteunend Onderwijzend Personeel
OP	Onderwijzend Personeel
VOG	Verklaring Omtrent Gedrag, is een standaard in het aannameproces voor medewerkers
Wbp	Wet bescherming persoonsgegevens (1995), voorloper van de AVG
WHW	Wet Hoger- en Wetenschappelijk onderwijs, van toepassing voor de hogeschool
WOT	Wet Onderwijs Toezicht, van toepassing bij School Voor Jong Talent.
WPO	Wet op Primair Onderwijs, van toepassing bij School Voor Jong Talent.
WVO	Wet op Voortgezet Onderwijs, van toepassing bij School Voor Jong Talent.

Bijlage B: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht. Deze lijst kan en mag verder worden uitgebreid.

Richtlijn:	**Beschikbaarheid**
Gebruik Persoonsgegevens	Intranet
Privacy statement MDW, STUD	Intranet, aanstelling, aanmelding
Privacy statement gasten, bezoeker	Intranet
Bewaartermijnen	Intranet
Gebruik ICT en internet	Intranet
Acceptable use policy	Intranet
Gebruik Bring Your Own Device	Intranet
Procedures	
Toestemming gebruik persoonsgegevens	Intranet
Gebruik beeldmateriaal	Intranet
Gebruik cameratoezicht	Intranet
Gebruik social media	Intranet
Verwijderen van persoonsgegevens	Intranet
Proces Privacyrecht	Intranet
Proces autorisatiematrix	Intranet
Training en awareness	Intranet
Wachtwoordenbeleid	Intranet
Delen van persoonsgegevens	Intranet
Verloren voorwerpen	Intranet
Security procedures	Intranet
Registers	
Verwerkingsregister	IBP-team
Toestemmingsregister(s)	IBP-team
Verwerkersovereenkomsten register	IBP-team
Incidenten register	IBP-team
Autorisatie register(s)	IBP-team, ICT, afdelingshoofden
Privacy Impact Assessments	IBP-team, ICT, afdelingshoofden
Monitoring logs	ICT