Beleid Informatiebeveiliging en Privacy

Koning Willem I College

Inhoud

Inleiding
Binnen het KW1C staat de student centraal en is ons uitgangspunt. Het belang van de student staat voorop, of het nu een initiële student, een zij-instromer of een student met extra ondersteuningsbehoefte is. Het leren van de student is bij ons gericht op de praktijk én vindt plaats in de praktijk, op één of meer van onze locaties in Noordoost-Brabant die het beste passen bij de toekomst van de individuele student. Altijd in een veilige omgeving, waar je mag zijn wie je bent.
In dit beleid, ingegaan op 1 augustus 2023, wordt weergegeven hoe de informatiebeveiliging en privacybescherming binnen het KW1C is ingeregeld. Het beleid geeft richtlijnen en kaders voor het ontwerpen van procedures en werkwijzen. Het biedt handvaten aan medewerkers en studenten om de continuïteit van het onderwijs en de bedrijfsvoering te waarborgen, om de privacy van alle betrokkenen van wie het KW1C persoonsgegevens verwerkt te garanderen en om beveiligings- en privacy-incidenten te voorkomen en de eventuele gevolgen hiervan te beperken.

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

- Wet Educatie en Beroepsonderwijs (WEB);
- Branche code Goed Bestuur MBO, MBO Raad;
- Wet op het Onderwijstoezicht;
- Algemene verordening gegevensbescherming (AVG);
- Archiefwet;
- Auteurswet;
- Wetboek van Strafrecht;
- Koppelingswet.

Het NBA (Nederlandse Beroepsvereniging van Accountants) toetsingskader is leidend voor de te nemen beveiligingsmaatregelen.

Het KW1C hanteert het Toetsingskader NBA en Privacy dat ontwikkeld is door MBO-Raad (MBO Digitaal).

1. Verantwoording en richtlijnen

1.1 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, met name ook van minderjarigen[1].De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. 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.

Dit IBP-beleid beschrijft en onderbouwt de basisafspraken waar we binnen KW1C met elkaar verantwoordelijk voor zijn en conform naar werken.

1.2 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 volledig, juist en actueel 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 het KW1C. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades, boetes en imagoverlies.

1.3 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens over een geïdentificeerd of identificeerbaar natuurlijk persoon. Een persoonsgegeven kan direct of indirect herleidbaar zijn tot een persoon.

De definitie van een persoonsgegeven is daarmee zeer breed ingestoken. Het gaat niet alleen om gegevens die direct herleidbaar zijn tot een persoon, zoals een naam, een e-mailadres of een geboortedatum. Ook gegevens die indirect of in combinatie met andere gegevens herleidbaar zijn tot een persoon, zijn aan te merken als persoonsgegeven. Te denken valt dan bijvoorbeeld aan een IP-adres, een postcode of een cookie-ID. Zolang het, op welke manier dan ook, mogelijk is om te achterhalen van wie de gegevens zijn, vallen deze gegevens onder de definitie van een persoonsgegeven onder de AVG.

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].

[1] Groene woorden worden in bijlage 1 (Verklarende woordenlijst) toegelicht.

[2] Bewerkt artikel 2, lid 2 van de AVG.

1.4 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor de bescherming van persoonsgegevens, 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 geheel: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis voor informatiebeveiliging en de bescherming van persoonsgegevens binnen het KW1C en vormt de kapstok voor de onderliggende afspraken en processen hiervoor.

1.5 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 van wie het KW1C persoonsgegevens verwerkt, waaronder studenten, hun ouders/verzorgers en medewerkers.
- Beveiligings- 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. van medewerkers, studenten en hun ouders/verzorgers) wordt gerespecteerd en het KW1C voldoet aan relevante wet- en regelgeving.

1.6 Reikwijdte

- Het IBP-beleid binnen het KW1C geldt voor alle betrokkenen, te weten: medewerkers (in de breedste zin van het woord), studenten, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing).
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van het KW1C. 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 (b.v. uitspraken van medewerkers, op (persoonlijke pagina's van) websites en of social media). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van het KW1C evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid 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.

Het IBP-beleid heeft binnen het KW1C raakvlakken met:
• *Het algemeen veiligheidsbeleid*; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen.
• *Het personeels- en organisatiebeleid*; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.
• *Het IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen.
• De medezeggenschap van studenten, hun ouders/verzorgers en medewerkers.

1.7 Concretisering

Het KW1C hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het College van Bestuur van het KW1C 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.

2. Het KW1C voldoet aan alle **relevante wet- en regelgeving**, zie paragraaf 2.1.

3. Bij het KW1C 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 het KW1C 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 intrekken of herzien.

4. Het KW1C 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 de rechten die zijn hebben met betrekking tot hun persoonsgegevens. Te weten:
    a. Het recht op informatie;
    b. Het recht op inzage;
    c. Het recht op verbetering;
    d. Het recht op verwijdering;
    e. Het recht op beperking van de verwerking;
    f. Het recht op bezwaar;
    g. Het recht op overdraagbaarheid van de gegevens (dataportabiliteit);
    h. Het recht om niet onderworpen te worden aan een uitsluitend geautomatiseerde besluitvorming, waaronder profilering.

Voor meer informatie over de rechten van betrokkenen en hoe het KW1C omgaat met verzoeken van betrokkenen tot de uitoefening van één van hun rechten, zie het ‘Protocol rechten van betrokkenen’.

5. Het KW1C legt alle **verwerkingen van persoonsgegevens** vast in een dataregister en zal deze up-to-date houden. Het KW1C voldoet hiermee aan de documentatieplicht, zoals benoemd in de AVG.

6. Binnen het KW1C is **het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van eenieder**. Hierbij hoort:

    1. het actief bijdragen aan de veiligheid van geautomatiseerde systemen en daarin opgeslagen informatie; onder ander door middel van het afsluiten van de computer als de werkplek verlaten wordt (clear screen policy).
    2. het veilig bewaren van papieren documenten en op de werkplek geen papieren documenten achterlaten zodra deze verlaten wordt (clear desk policy).

7. Het KW1C 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 studenten worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. Het KW1C **classificeert informatie**. 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.

9. Het KW1C sluit met **alle leveranciers van digitale onderwijsmiddelen** (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken.

10. Het KW1C verwacht van **alle medewerkers, studenten, (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. KW1C heeft hiervoor een **gedragscode** geformuleerd, vastgesteld en geïmplementeerd.

11. **Informatiebeveiliging en privacy is bij het KW1C een continu kwaliteitsproces**, waarbij regelmatig (minimaal jaarlijks) wordt ge-audit of een self assessment wordt uitgevoerd en wordt gekeken of een aanpassing gewenst dan wel noodzakelijk is.

12. Het KW1C kijkt bij **wijzigingen** (denk ook aan uitfasering) 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.

13. Het KW1C neemt **passende organisatorische of 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.

14. Het KW1C zal alle beveiligingsincidenten en datalekken, volgens een vast protocol vastleggen, afhandelen en indien van toepassing melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

15. Het KW1C kiest ten aanzien van informatiebeveiliging (autorisatie en authenticatie) voor de vooronderstelling "Alles is in principe verboden tenzij het uitdrukkelijk is toegelaten"[3] in plaats van de zwakkere regel "Alles is in principe toegelaten tenzij het uitdrukkelijk is verboden".

16. Het is medewerkers van het KW1C niet toegestaan om zonder toestemming van de direct leidinggevende schooleigendommen mee te nemen naar een locatie buiten het KW1C. Denk hierbij aan apparatuur zoals PC's, printers en Digiborden.

17. Bij het verlaten van de werkplek zorgt de medewerker ervoor dat zijn bureau schoon is en het beeldscherm is vergrendeld.

18. Indien een medewerker thuis werkt, worden dezelfde IBP-richtlijnen in acht genomen als op de werkplek bij het KW1C, zie ook het Thuiswerkbeleid.

[3] Op basis van functie/rollen worden rechten door de leidinggevende toegekend. Een functioneel beheerder kent de rechten feitelijk toe. Bijvoorbeeld: een HR adviseur mag alleen de dossiers van de aan hem/haar toegewezen medewerkers inzien, als dat noodzakelijk is vanwege de opgedragen werkzaamheden.

2. Compliance

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

2.1 Relevante wet- en regelgeving

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

- Wet Educatie en Beroepsonderwijs (WEB);
- Branche code Goed Bestuur MBO, MBO Raad;
- Wet op het Onderwijstoezicht;
- Algemene verordening gegevensbescherming (AVG);
- Archiefwet;
- Auteurswet;
- Wetboek van Strafrecht;
- Koppelingswet.

Het NBA (Nederlandse Beroepsvereniging van Accountants) toetsingskader is leidend voor de te nemen beveiligingsmaatregelen.

Het KW1C hanteert het Toetsingskader NBA en Privacy dat ontwikkeld is door MBO-Raad (MBO-Digitaal).

2.2 Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake de verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de **zes 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, inclusief de bewaartermijnen. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **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 (subsidiar).
3. **Opslagbeperking**: Persoonsgegevens blijven niet langer bewaard dan noodzakelijk is voor het doel waarvoor de gegevens verzameld zijn.
4. **Rechtmatigheid, behoorlijkheid en transparantie**: het KW1C draagt er zorg voor dat zij zich bij de verwerking van persoonsgegevens houdt aan de wet. Zo verwerkt zij enkel persoonsgegevens als zij hier een grondslag voor heeft, zoals genoemd in de AVG. Bovendien is het KW1C als verwerkingsverantwoordelijke verplicht om betrokkenen (studenten, hun ouders en medewerkers) op transparante wijze te informeren over het gebruik van hun persoonsgegevens. Deze informatievoorziening vindt ongevraagd en voorafgaand aan de verwerking plaats. Aan de informatieverplichting wordt voldaan middels een privacy(- en cookie)verklaring, waarin opgenomen is welke persoonsgegevens verwerkt worden, waarom zij verwerkt worden en hoe.
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens volledig, juist en actueel zijn[4].
6. **Integriteit en vertrouwelijkheid**: Het KW1C neemt passende technische en organisatorische maatregelen om de persoonsgegevens welke zij verwerkt tegen verlies of enige andere vorm van onrechtmatige verwerking te beschermen. Daarbij houdt zij rekening met de stand van de techniek en de gevoeligheid van de persoonsgegevens die verwerkt worden.

[4] Bij Data-integriteit is veilig en discreet omgaan met de toevertrouwde persoonsgegevens uitgangspunt.

2.3 Ondersteunende richtlijnen en procedures
Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in dataregisters. Bijlage 2 geeft een overzicht van de diverse aanvullende documenten die gepubliceerd worden op het KW1C intranet.

2.4 Classificatie en risicoanalyse
Alle gegevens en informatiesystemen waarop dit beleid van toepassing is worden 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 kwaliteitscriteria 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 middels een centraal ingeregeld DPIA (Data Protection Impact Assessment). Vanaf de start van elk nieuw project wordt rekening gehouden met informatiebeveiliging en privacy.

2.5 Beveiligingsincidenten en datalekken
Alle medewerkers en studenten die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. Bij de afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings-)incidenten dienen gemeld te worden bij de IT-servicedesk.

De (beveiligings-)incidenten worden vastgelegd in een incidentenregister en worden periodiek besproken binnen de IBP-organisatie. Waar nodig zullen aanvullende passende beleidsmaatregelen genomen worden.

2.6 Planning en controle
Dit IBP-beleid wordt jaarlijks gereviewed en eventueel bijgesteld in opdracht van het College van 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 het KW1C een jaarlijks verbeterplan voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het IBP-beleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

2.7 Naleving en sancties
De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Naleving van ons IBP-beleid is een primaire verantwoordelijkheid van alle medewerkers binnen het KW1C. Daar boven nemen de leidinggevenden en proceseigenaren hun verantwoordelijkheid om hun medewerkers aan te spreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP-zaken bij de aanstelling, tijdens functioneringsgesprekken, d.m.v. een instelling brede gedragscode, periodieke bewustwordingscampagnes, et cetera.

Voor toezicht op de naleving van de AVG vervult de FG een belangrijke rol. De FG wordt aangesteld door het College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan het KW1C de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

2.8 Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt er voor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens worden vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk. Het KW1C beoordeelt deze logbestanden met regelmaat.

2.9 Voorlichting en Bewustzijn

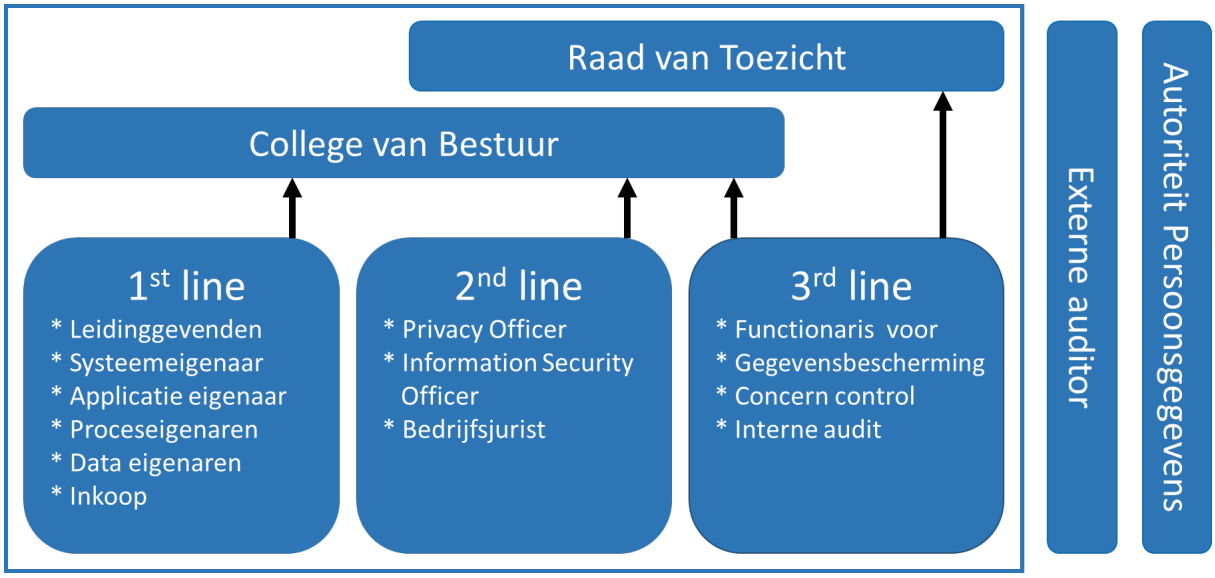
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacybescherming uit te sluiten. De mens is tenslotte een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de Beleidsgroep IBP, de Functionaris voor Gegevensbescherming (FG)-Privacy Officer (PO)-Information Security Officer (ISO) met het College van Bestuur als eindverantwoordelijke.

Iedere medewerker ontvangt op regelmatige basis bijscholing op het gebied van informatiebeveiliging en privacybescherming.

3. Governance

3.1 Rollen en verantwoordelijkheden

Koning Willem I College hanteert het three lines model. De eerste lijn binnen dit model is cruciaal, immers de leidinggevenden moeten er op toezien dat de AVG wordt nageleefd. Daartoe zijn alle managers geschoold en zij zien erop toe dat al hun teamleden handelen volgens het vastgesteld IBP beleid. Schematisch als volgt weergegeven.



3.2 De first line: Leidinggevenden, Systeemeigenaar, Applicatie eigenaar, Proceseigenaren, Dataeigenaren en Inkoop

Leidinggevenden (Cruciale rol 1e lijn)

De eerste lijn is verantwoordelijk voor de volgende onderwerpen:

1. Eigen scholing.
2. Scholing toegewezen leidinggevenden / medewerkers (inclusief awareness).
3. Naleving afspraken (voorkomen schaduwadministraties).
4. Registreren toegekende extra autorisaties.
5. Toezien op verwerkersovereenkomsten van decentrale applicaties die gebruikt worden binnen hun organisatorische eenheid.

Systeem-eigenaar

De systeemeigenaar is eigenaar van alle componenten (zowel hard- als software) in het ICT netwerk.

Applicatie-eigenaar

Binnen het KW1C is de systeem-eigenaar tevens de applicatie-eigenaar. De applicatie eigenaar is verantwoordelijk voor:

1. Inrichten van de applicatie conform de eisen van het IBP-beleid.
2. Vaststellen van een autorisatiematrix en een passende toegangsverleningsprocedure.
3. In samenspraak met de proces-eigenaar vaststellen van de rollen en rechten van medewerkers.
4. Toezien op leveranciersmanagement, waaronder het jaarlijks beoordelen van de verwerkersovereenkomst en beveiligingsaspecten, ondersteund door de afdeling Inkoop.
5. Periodiek laten uitvoeren van een data protection impact assessment, indien dit noodzakelijk is conform wetgeving.

Proceseigenaren
De proceseigenaren worden door het College van Bestuur benoemd. De proceseigenaar zal in overleg met de applicatie-eigenaar de processen laten inrichten, doorgaans met behulp van applicaties waarvan hij de functionaliteit mee heeft bepaald.
De proces-eigenaar is daardoor ook verantwoordelijk voor bijvoorbeeld de inrichting van het systeem op basis van de principes uit dit beleid. Dit betekent bijvoorbeeld concreet dat de proces-eigenaar verantwoordelijk is voor het vaststellen van rollen en rechten en de toetsing op need-to-know en dataminimalisatie binnen zijn proces en de bijbehorende applicaties.
De processen zoals opgenomen in de MORA (Middelbaar beroepsOnderwijs Referentie Architectuur) zijn leidend.

Data eigenaren
De data eigenaar is eigenaar van de persoonsgegevens (kroonjuwelen) zoals vermeld in de procesdataregisters.
KW1C hanteert de term kroonjuwelen. Binnen het onderwijs zijn er 4 kroonjuwelen, te weten:

1. Medewerkersgegevens;
2. Studentengegevens;
3. Examengegevens;
4. Financiële gegevens.

De data eigenaar “leent” de data uit aan de organisatorische eenheden die, vervolgens, deze data mogen aanvullen met relevante data. Als de betrokkene (medewerker of student) de onderwijsinstelling verlaat dan worden de data teruggeven aan de data eigenaar die ze dan vervolgens zal archiveren of verwijderen.

De functioneel beheerder (geen onderdeel van 1e lijn)
Bundelt de rechten in een systeem tot een systeemrol en volgt procedures conform het inrichting- of beheerdocument voor die applicatie. De rechten op functionaliteiten en specifieke data worden vastgelegd in de autorisatiematrix. Op verzoek van leidinggevenden worden deze rollen aan specifieke medewerkers toegekend.
De functioneel beheerder van een applicatie zorgt voor actuele autorisatiematrix, waarin is opgenomen welke rollen en rechten er zijn binnen de desbetreffende applicatie.

Periodieke controle
De leidinggevende is verantwoordelijk voor de uitgifte van rollen en rechten van haar medewerkers. De leidinggevende dient periodiek (minimaal 1x per jaar) te controleren of de uitgegeven rollen/rechten nog actueel zijn, de systeem-eigenaar faciliteert hiervoor een proces.

Samenhang tussen de rollen binnen het IBP beleidsplan van het KW1C.

Rol	Toewijzing	Invulling
Systeemeigenaar	Directeur Informatievoorziening	Aanbesteding en kostenplaatseigenaar en contracteigenaar van systemen (hardware en applicaties)
Applicatie eigenaar	Directeur Informatievoorziening	Eduarte HR2day Exact Office 365
Proceseigenaar	Managers benoemd op basis van de MORA architectuur	

3.3 De second line: IBP-organisatie en de bedrijfsjurist van het KW1C
Experts op het gebied van informatiebeveiliging en privacybescherming monitoren de toepassing en naleving van het informatiebeveiligings- en privacy beleid. Zij adviseren, gevraagd en

ongevraagd, over informatiebeveiliging en privacybescherming en ondersteunen de first line, bijvoorbeeld met het afsluiten van overeenkomsten met derde partijen.

De IBP-organisatie ontwikkelt waar nodig beleid op het gebied van informatiebeveiliging en privacy, het College van Bestuur stelt dit voorgenomen beleid vast. De medewerkers van de IBP-organisatie vormen samen met de bedrijfsjurist de second line als het gaat om de bescherming van persoonsgegevens.

3.4 De third line: de Functionaris voor Gegevensbescherming, (interne) audit en Concern control

a) Functionaris voor gegevensbescherming
Het KW1C heeft een toezichthouder op de verwerking van persoonsgegevens aangesteld: de FG. De FG zal door het KW1C tijdig worden betrokken bij alle aangelegenheden waar persoonsgegevens bij komen kijken. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie binnen het KW1C. Het KW1C heeft de FG aangemeld bij de nationale toezichthoudende autoriteit, de Autoriteit Persoonsgegevens.
De taken van de FG houden in:

- Het informeren en adviseren van alle betrokken partijen over hun verplichtingen onder de AVG.
- Het toezien op de naleving van de AVG en andere relevante privacywetgeving.
- Het toezien op de naleving van dit IBP-beleid door KW1C.
- Het toezien op de inzet en uitvoering van Data Protection Impact Assessments.
- Het behandelen van klachten over de toepassing van het privacyreglement.
- Fungeren als eerste aanspreekpunt voor en samenwerken met de Autoriteit Persoonsgegevens.

b) (Interne) audit

- Het KW1C hanteert het NBA (Nederlandse Beroepsvereniging van Accountants) toetsingskader als (zelf) assessment tool.
- Jaarlijks vinden audits plaats waar de informatiebeveiliging en privacy getoetst worden door interne en/of externe auditors.

c) Concern control
Externe controles worden uitgevoerd door onafhankelijke accountants. Deze worden gepland en geformuleerd door Concern control van het KW1C.

3.5 Implementatie beleid

Het College van Bestuur van het KW1C is verantwoordelijk voor de verwerkingen van persoonsgegevens waarvoor zij doel en middelen vaststelt. Het College van Bestuur wordt aangemerkt als de verwerkingsverantwoordelijke in de zin van de AVG.

De verantwoordelijkheid houdt kort samengevat in:

- Dat de persoonsgegevens verwerkt worden in overeenstemming met de vastgestelde doelen van de verwerking, dat die doelen gerechtvaardigd zijn en dat de verwerking zorgvuldig gebeurt.
- Dat hierover verantwoording kan worden afgelegd aan de Autoriteit Persoonsgegevens.

De feitelijke verwerking van persoonsgegevens wordt echter op allerlei lagen van KW1C uitgevoerd. Het is niet één instituut of dienst die effectief verantwoordelijk kan zijn voor alle persoonsgegevens die het KW1C verwerkt. Er is een onderscheid tussen centrale verwerkingen, waarvoor de ondersteunende afdelingen verantwoordelijk zijn, en, aanvullend daarop, decentrale verwerkingen, waarvoor het onderwijsteam of dienst zelf verantwoordelijk is.

3.6 Taken van de medewerkers

(❶, ❷, ❸, ❹ en ❺ zijn de volgordelijke stappen)

Onderwerp	1 st line	2 nd line	3 rd line
Autorisaties	Functioneel beheerders brengen (in opdracht van proceseigenaren) autorisaties in kaart (IST) en toetsten dit bij het Management (SOLL). ❶ (stap 1)	De IBP-organisatie controleert of het SOLL en IST autorisatie vergelijk is uitgevoerd. ❷ (stap 2)	De FG controleert of de autorisaties zijn ingericht op basis van need-to-know en least privilege. ❸ (stap 3)
Beleidsdocumenten	Eerstelijnsleidinggevenden zien er op toe dat de goedgekeurde kaders en richtlijnen uit de beleidsdocumenten worden uitgevoerd. ❷	De IBP-organisatie schrijft en evalueert de beleidsdocumenten en bespreekt deze met de Beleidsgroep IBP en dient ze in bij het CvB ter goedkeuring. ❶	De FG toetst de kwaliteit van het beleid en de werking van het door het CvB goedgekeurde beleid. ❸
Bewaartermijn	Studentenadministratie en HR zijn verantwoordelijk voor het handhaven van de bewaartermijnen conform het Documentair Structuur Plan (DSP). ❶	De IBP-organisatie adviseert aan de hand van het Documentair Structuur Plan (DSP) de 1 st line over de geldende bewaartermijnen. ❷	De FG ziet er op toe dat de bewaartermijnen worden nageleefd. ❸
Bewustwording	Management voert het opleidingsplan van de IBP organisatie uit of stellen een afgeleid opleidingsplan vast. ❷	De IBP-organisatie stelt een opleidingsplan op voor IBP scholings- en awareness plannen en faciliteert ook centrale trainingen. ❶	De FG toetst het gewenste kennisniveau aan de scholings- en awareness plannen en komt eventueel met aanbevelingen. ❸
DPIA's	• Directeur, onderwijsmanager, teammanager, Inkoop, FB, IV en projectleiders voeren een pré DPIA uit bij ieder nieuw (ICT)project. ❶ • Directeur, onderwijsmanager, teammanager, FB, IV en projectleiders voeren een DPIA uit in opdracht van de FG. ❹	De IBP-organisatie komt op basis van de pré DPIA, uitgevoerd door de 1 st line, tot een voorstel om al dan niet een DPIA uit te voeren en wordt betrokken bij de uitvoering van de DPIA. ❷	De FG besluit op basis van het voorstel van de IBP organisatie of er een DPIA moet worden uitgevoerd en adviseert gevraagd en ongevraagd over de DPIA. ❸ De DPIA wordt slechts vastgesteld na goedkeuring van de FG. ❺
Datalekken	Medewerkers melden zelf intern een datalek via een registratiesysteem. Het management draagt zorg voor bekendheid van de meldprocedure en scholing van haar medewerkers. ❶	De PO beoordeelt de melding conform "Beleid melding datalekken". ❷	De FG adviseert het CvB om al dan niet het datalek bij de AP en/of de betrokkenen te melden. ❸ Als besloten wordt te melden, zorgt de FG dat deze melding tijdig en volledig plaatsvindt. ❹
Procesdataregisters centraal	De in § 3.2 aangewezen data-eigenaren voor de procesadataregisters bewaken de actualiteit van het dataregister. ❶	De IBP-organisatie adviseert en controleert op volledigheid, juistheid en actualiteit van de procesdataregisters. ❷	De FG toetst of het procesdataregister voldoet aan wet- en regelgeving. ❸
Door het management aangewezen uitvoerders	Het management wijst de deelprocesuitvoerders aan (bijv. examinering, roostering, stage, etc.). ❶	De IBP-organisatie toetst het toegewezen eigenaarschap aan de autorisatie. ❷	De FG toetst of het eigenaarschap beschreven is. ❸
Rechten van de betrokkenen	Medewerkers/studenten doen een verzoek aan de desbetreffende afdeling. Deze informeert de PO welke het verzoek in behandeling neemt (controle bij afdeling Studentadministratie of afdeling HR). ❶	De PO volgt de vastgestelde procedure en informeert de IBP-organisatie en de FG over het aantal verzoeken. ❷	De FG toetst of de vastgestelde procedure juist is gevolgd. ❸

Verwerkersover-eenkomsten	Inkoop en de IBP organisatie controleren middels de checklist of er een verwerkersovereenkomst is. Inkoop zorgt dat er altijd een verwerkersovereenkomst is opgesteld en kan de IBP organisatie om advies vragen. De IBP-organisatie stuurt de verwerkersovereenkomst ter goedkeuring naar de FG. ❶	De IBP-organisatie adviseert bij verwerkersovereenkomsten op verzoek van de 1 st line. ❷	De PO toetst de verwerkersovereenkomst op rechtmatigheid en volledigheid. Het College van Bestuur tekent de verwerkersovereenkomst na akkoord van de PO. De FG toetst op regelmatige basis. ❸
Vragen van medewerkers betreffende IBP gerelateerde onderwerpen	Het management is het eerste aanspreekpunt voor vragen inzake privacy en security, medewerkers kunnen de IBP-organisatie ook zelf benaderen. ❶	De IBP-organisatie adviseert de manager en/of medewerker. ❷	De FG controleert de gestelde vragen en de oplossingen. ❸

3.7 Verdeling van de verantwoordelijkheden

Het KW1C onderscheidt een drietal soorten verwerkingen van persoonsgegevens met daarbij benoemde broneigenaren (tevens data-eigenaren):

- De Studentenadministratie (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle personen die bij het KW1C onderwijs volgen. De Studentenadministratie is verantwoordelijk voor de procesdataregisters: Student en Student tijdelijk niet actief.
- HR (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle personen die in opdracht van het KW1C, zowel centraal als decentraal, werk verrichten. HR is verantwoordelijk voor de procesdataregisters: Medewerkers in loondienst en Medewerkers niet in loondienst.
- De opdrachtgever van onderzoek (broneigenaar) dat het KW1C uitvoert, zowel centraal als decentraal, is verantwoordelijk voor de verwerkingen van persoonsgegevens in het kader van dat onderzoek. Een onderzoeksvoorstel wordt altijd voorgelegd aan de IBP-organisatie en getoetst door de FG.

Er worden geen persoonsgegevens verwerkt buiten de verantwoordelijkheid van een van bovengenoemde broneigenaren, tenzij dit met toestemming gebeurt. Het KW1C bepaalt op welke manier deze verwerkingen worden gedocumenteerd. De FG geeft als toezichthouder gevraagd en ongevraagd advies.

3.8 Inpassing in instellingsgovernance en afstemming met aanpalende beleidsterreinen

Om de samenhang in de organisatie met betrekking tot gegevensbescherming goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van verwerking van persoonsgegevens binnen de verschillende onderdelen op elkaar af te stemmen, is het belangrijk om gestructureerd overleg te voeren over het onderwerp privacy op verschillende niveaus.
Op **strategisch niveau** wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van privacyaspecten. Het strategisch niveau wordt voorbereid door de 2e en 3^{e} lijn.
Op **tactisch niveau** wordt de strategie vertaald naar plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering. Het tactisch niveau wordt ingevuld door de 2^{e} lijn.
Op **operationeel niveau** worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan. Het operationeel niveau wordt ingevuld door de eerstelijnsleidinggevenden zowel op centraal als decentraal niveau.

3.9 Richtlijn IBP-netwerk

In het kader van IBP is het van belang dat de betrokken functionarissen aangesloten zijn bij diverse landelijke netwerken:

- De FG is geregistreerd bij het Nederlands Genootschap van Functionarissen voor Gegevensbescherming en aangesloten bij het Netwerk IBP in het MBO van MBO-Digitaal en het netwerk IBP van Kennisnet.
- De PO is aangesloten bij het Netwerk IBP in het MBO van MBO-Digitaal en bij de SCIPR en SCIRT communities van SURF .
- De ISO is aangesloten bij het Netwerk IBP in het MBO van MBO-Digitaal, eventueel bij de Koninklijke Vereniging van Informatieprofessionals, bij het Platform voor Informatie Beveiliging en bij de SCIPR- en SCIRT communities van SURF.

3.10 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Noodzakelijk is het om het bewustzijn voortdurend aan te scherpen, zodat bij het KW1C de bewustwording van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn workshops voor medewerkers en regelmatig terugkerende bewustwordings-campagnes voor medewerkers, studenten en relaties. Verhoging van het bewustzijn is de verantwoordelijkheid van elke leidinggevende en wordt gefaciliteerd door de IBP-organisatie.

3.11 Controle en naleving

Audits en assessments maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert gezamenlijk met de 2e lijn en de interne auditfunctie de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens.

Eventuele externe controles worden uitgevoerd door onafhankelijke accountants. Deze externe controles worden gepland en geformuleerd in een nauwe samenspraak met de interne auditfunctie van het KW1C.

Mocht de naleving op de bescherming van (persoons)gegevens ernstig tekortschieten, dan kan het KW1C de betrokken verantwoordelijke medewerkers een maatregel opleggen, binnen de kaders cao-mbo en de wettelijke mogelijkheden.

Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten het KW1C maken het noodzakelijk om periodiek te beoordelen of men nog voldoende op koers zit met het beleid.

Dit IBP-beleid wordt derhalve jaarlijks opnieuw beoordeeld en aangepast indien nodig.
Mochten bijvoorbeeld wettelijke bepalingen dit vereisen, kan een herbeoordeling eerder plaats vinden.

Besluiten in het kader van dit IBP-beleid worden opgenomen in een separate besluitenlijst

Bijlage 1: Verklarende woordenlijst

AVG: Algemene verordening gegevensbescherming.

Beleid: Beleid met betrekking tot het verwerken van persoonsgegevens door het KW1C.

Betrokkene: Een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft.

Broneigenaar: Aangewezen directeur die verantwoordelijk is voor persoonsgegevens van één of meerdere categorieën van Betrokkenen. De Broneigenaar voert de persoonsgegevens in en zorgt voor de vernietiging. In de tussentijd leent hij ze uit aan de organisatorische eenheden binnen het KW1C. De organisatorische eenheden mogen dan de persoonsgegevens verrijken.

Datalek: Een inbreuk in verband met persoonsgegevens, die leidt tot enige ongeoorloofde verwerking daarvan. Hier vallen zowel opzettelijke als onopzettelijke inbreuken onder.

Dataportabiliteit: Het recht om persoonsgegevens en informatie over te dragen aan een andere partij zonder technische problemen.

Dataregister: De AVG spreekt van het Register van Verwerkingsactiviteiten, dit is een overzicht van de persoonsgegevens die verwerkt worden, met informatie over het doel daarvan, de grondslag daarvoor, de bewaartermijnen van de gegevens en bron of ontvanger van de gegevens. Het KW1C heeft drie centrale registers: dat voor studentgegevens, voor medewerker gegevens en voor relatiegegevens. Het dataregister is het Register van Verwerkingsactiviteiten aangevuld met de BIV-classificatie en de autorisatie matrix op hoofdlijnen.

DPIA: Data Protection Impact Assessment (Gegevensbeschermingseffectbeoordeling): een beoordeling die helpt bij het identificeren van privacy risico's en de handvatten levert om deze risico's te verkleinen tot een acceptabel niveau. Soms ook wordt de term PIA gebruikt, Privacy Impact Assessment.

Functionaris voor Gegevensbescherming: Interne toezichthouder en privacy adviseur aangesteld door het College van Bestuur, op grond van artikel 37 van de AVG, ook wel aangeduid als FG.

Kernsystemen: De hoofdsystemen voor: SIS, HR, Financiën, Rooster, ELO, MIS, CRM, IDM, Office en ARBO.

Minderjarige: Voor de AVG geldt: iedere persoon die de leeftijd van 16 jaar nog niet heeft bereikt. Buiten de AVG geldt: iedere persoon jonger dan 18 jaar.

Niet-geautomatiseerde verwerking: Voorbeelden: aangetekende stukken, pasjes die zichtbaar gedragen worden, klassenlijsten met foto's (smoelenboek), etc.

Persoonsgegeven: Elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon.

Privacy by Default: Een gegevensverwerking waarbij de standaardinstellingen van producten en diensten zo zijn ingesteld dat de privacy van betrokkenen maximaal wordt gewaarborgd. Dit betekent onder meer dat er zo min mogelijk gegevens worden gevraagd en verwerkt.

Privacy by Design: Al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) wordt ten eerste aandacht besteed aan privacy verhogende maatregelen. Ten tweede wordt rekening gehouden met dataminimalisatie: er worden zo min mogelijk persoonsgegevens verwerkt, alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.

Verwerker: Een door het KW1C ingeschakelde (derde) partij die ten behoeve van het KW1C, en op basis van haar schriftelijke instructies, persoonsgegevens verwerkt, e.e.a. vastgelegd in een verwerkersovereenkomst.

Verwerking: Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, afschermen, wissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke: Het College van Bestuur van het KW1C dat het doel en de middelen van de verwerking van persoonsgegevens vaststelt.

Bijlage 2: Gehanteerde referentiedocumenten

Dit beleid wordt verder uitgewerkt in de volgende documenten:

Referentiedocumenten Governance:
NBADOC G01-Strategie
NBADOC G01-Strategie Audit
Voor KW1C is Informatiebeveiliging en Privacy essentieel voor de continuïteit, kwaliteit en veiligheid van het onderwijs. Dit sluit aan bij de volgende strategische uitgangspunten: toekomstbestendig onderwijs; professionele (onderwijs)organisatie; intrinsieke leer- en verbetercultuur en een sterke organisatie.
KW1C biedt een veilige en professionele leer- en werkomgeving aan. Daarbij zijn de door KW1C verzamelde, verwerkte en gepubliceerde informatie te allen tijde beschikbaar, correct en beschermd. Dit vraagt om een strategisch samenhangende aanpak van Informatiebeveiliging en Privacy, die aantoonbaar aan de eisen voldoet, om blijvend een veilige en toekomstbestendige leer- en werkomgeving beschikbaar te stellen.

NBADOC G02-Beleid
NBADOC G02-Beleid Audit
Door het College van Bestuur is een nieuwe versie van het Informatiebeveiliging en privacy beleid vastgesteld. Of de beschrijving van rollen en verantwoordelijkheden aansluit bij de situatie binnen KW1C zal moeten worden geëvalueerd. Tevens zal op termijn meer verwezen moeten gaan worden naar andere beleidstukken die bij de implementatie van het NBA-model vastgesteld zullen gaan worden.

NBADOC G03-Architectuur
NBADOC G03-Architectuur Audit
Werken vanuit een vastgesteld architectuur geeft duidelijkheid over waar welke informatie verwerkt wordt. Inzicht in het applicatielandschap en procesmatig werken zijn noodzakelijk om Informatiebeveiliging en Privacy te kunnen borgen in de hele organisatie.
KW1C heeft het architectuurmodel MORA formeel vastgesteld als uitgangspunt voor de processen die we binnen onze organisatie hanteren. In het referentiedocument worden de statements van het NBA-model geplot op de MORA. Niet alle statements komen voor in het MORA-model, maar het is de bedoeling dat ze daarin wel opgenomen worden, evenals de BIV-classificatie van elk proces.

NBADOC G04-Eigenaarschap
NBADOC G04-Eigenaarschap Audit
Het benoemen eigenaarschap met betrekking tot Informatiebeveiliging en Privacy is essentieel om Informatiebeveiliging en Privacy te borgen in heel de organisatie. Duidelijk is dat het College van Bestuur de eindverantwoordelijkheid draagt. Ook dragen we uit dat iedereen een verantwoordelijkheid heeft om veilig om te gaan met de informatie die ons is toevertrouwd. Voor het adresseren van eigenaarschap gebruikt KW1C het VERI-model. Hierin zijn de verschillende verantwoordelijkheden met betrekking tot de thema's ondergebracht.
De eigenaren (eindverantwoordelijke) zijn benoemd. De uitvoerders (verantwoordelijke) zijn deels benoemd en moeten in sommige gevallen nog worden aangewezen. Wie verder nog betrokken moeten worden (geraadpleegde/geïnformeerde) zal bij de uitvoering van de taken die genoemd zijn in de Roadmap verder worden ingevuld. Hierin zullen de Eindverantwoordelijken begeleid en getraind worden door de Information Security Officer met als doel concreet te gaan werken vanuit de vastgestelde Governance.

NBADOC G05-Risk Management
NBADOC G05-Risk Management Audit
KW1C volgt de risicoanalyse die gemaakt is vanuit het SURF Cyberdreigingsbeeld. Op basis daarvan zijn de volgende risico's benoemd:

R1: Governance niet op orde
R2: Aanval Ransomware
R3: Afhankelijkheid van Cloud Computing
R4: Identiteitsfraude
R5: Niet hanteren van Bewaartermijnen
Het risicoactieplan van KW1C richt zich op de in het NBA genoemde beheersmaatregelen van bovengenoemde risico's. In de Roadmap zijn deze acties gekoppeld aan tijdlijn en eigenaar.

NBADOC G06-Roadmap
NBADOC G06-Roadmap Audit
De Roadmap geeft het groeipad aan dat KW1C moet doorlopen om de genoemde risico's te mitigeren. Deze risico-gebaseerde aanpak prioriteert de beheersmaatregelen die in het NBA-model staan. Voor alle onderwijssectoren (PO, VO, mbo, HO en Uni) is volwassenheidsniveau 3 (opzet en bestaan) voor de meeste NBA-statements het gewenste niveau. KW1C onderschrijft dit en meent zelfs dat voor een groot aantal statements volwassenheidsniveau 4 haalbaar (en gewenst) is als de beheersmaatregelen goed geborgd worden in de manier van werken. Sturen op een reëel en een risico gebaseerd actieplan is hierin effectiever dan werken met een compleet uitgewerkte Roadmap.

NBADOC G07-Toetsing
NBADOC G07-Toetsing Audit
Sluitstuk van de Governance is de onafhankelijke toetsing. KW1C ziet dit niet als een (eind)examen maar vooral als instrument om de Informatiebeveiliging en Privacy op niveau te krijgen en houden. KW1C toetst (intern) en laat zich toetsen (extern).
Intern toetst de KW1C middels mini-assessments en DPIA's. Deze zijn opgenomen in de Roadmap. Een uitgebreidere interne audit wordt gedaan door de interne IT-auditor. Deze audit dient niet alleen om het College van Bestuur inzage geven over hoe de KW1C ervoor staat, maar ook als opmaat voor de externe toetsing en input voor de mbo Benchmark (hoe staan we er voor t.o.v. de andere onderwijsinstellingen).

Referentiedocumenten Processen:
NBADOC P08-Human Resources
NBADOC P08-Human Resources Audit
Betreft borging expertise en training.

NBADOC P09-ITIL
NBADOC P09-ITIL Audit
Betreft Incident, Problem, Change, en Configuration Management en Fysieke Beveiliging.

NBADOC P10-Data Management
NBADOC P10-Data Management Audit
Betreft opslag, beheer, verwijderen (bewaartermijnen) en bescherming van gegevens.

NBADOC P11-IAM
NBADOC P11-IAM Audit
Betreft toegangsregels en - rechten tot informatie.

NBADOC P12-Security Baselines
NBADOC P12-Security Baselines Audit
Minimale afspraken over hoe veilig te werken.

NBADOC P13-Business Continuity
NBADOC P13-Business Continuity Audit
Betreft opvangen van incidenten (waaronder crisismanagement).

NBADOC P14-Cloud Leveranciers (Ketenafhankelijkheid)

NBADOC P14-Cloud Leveranciers Audit
Goede afspraken en controle daarop bij externe leveranciers.

Referentiedocumenten Technische Weerbaarheid:
NBADOC T15-T21 Technische Weerbaarheid
NBADOC T15-T21 Technische Weerbaarheid Audit
Bij technische weerbaarheid zijn de volgende thema's te onderscheiden:

1. Multi Factor Authenticatie/Thuiswerken: betreft veilig van buitenaf inloggen.
2. SOC SIEM: betreft 24 x 7 detectie van het netwerk (en respons).
3. Pentesten: betreft periodiek gericht testen op kwetsbaarheden in het netwerk.
4. Patchbeheer: betreft structureel bijwerken van de software (beveiligingsupdates).
5. Infrastructuur: betreft beschikbaarheid van het netwerk en systemen.
6. Security Policy: betreft inrichting technische beveiliging van het netwerk en systemen.
7. Computer Operations: betreft automatische IT-processen (bijvoorbeeld back-up).

De bovenstaande thema's zullen uitgevoerd of onder regie uitbesteed worden door de IT-afdeling. Zij zullen hierover in begrijpelijke taal rapporteren aan het College van Bestuur. Bij deze rapportage hoort ook een financieel overzicht, zodat duidelijk is welke veiligheidsmaatregelen horen bij de gemaakt kosten/investeringen.
De thema's Multi Factor Authenticatie/Thuiswerken, SOC SIEM en Security Policy vallen onder het zogenaamde Zero Trust principe.

Bijlage 3: Ondersteunende documenten

Deze bijlage bevat een aantal aanvullende documenten. Een aantal zijn vanuit de AVG verplicht.

	IBP beleid 1.7 Concretisering:	KW1C document:	Bron:
1	College van Bestuur, verwerkingsverantwoordelijke	IBP-beleid KW1C, hoofdstuk 3	MBO-Raad
2	Relevante wet- en regelgeving	IBP-beleid KW1C, hoofdstuk 2	MBO-Raad
3	Specifiek doel en wettelijke grondslag	• Dataregisters • Toestemmingsverklaringen	• MBO-Raad • Eigen versie
4	Betrokkenen helder en actief informeren	Privacyregeling voor medewerkers en studenten	MBO-Raad
5	Verwerkingen van persoonsgegevens (dataregisters)	• Dataregisters medewerkers • Dataregister studenten • Dataregister relaties	MBO-Raad
6	Veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van eenieder	• Privacyreglement	• Goedgekeurd door OR • Goedgekeurd studentenraad
7	Eigendom toebehoort aan derden	Auteursrecht	MBO-Raad
8	Classificeren persoonsgegevens	BIV classificatie	MBO-Raad
9	Leveranciers van digitale onderwijsmiddelen	Model verwerkersovereenkomsten KW1C	MBO-Raad
10	Medewerkers, studenten, (geregistreerde) bezoekers en externe relaties gedragen zich ‘fatsoenlijk’	• Studenten statuut • AVG in het onderwijs • Reglement verantwoord computergebruik	• Eigen versie • Bewerkte versie SURF • Eigen versie
11	Informatiebeveiliging en privacy is een continu kwaliteitsproces	Self assessment op basis van ISO27001/2 en NBA	MBO-Raad
12	Wijzigingen en aanschaf van nieuwe (informatie)systemen	• Privacy by design/default • DPIA • OTAP beleid	• SURF • Rijksoverheid • Eigen versie
13	Passende organisatorische of technische (beveiligings-)maatregelen	DPIA, deel 2	Rijksoverheid
14	Beveiligingsincidenten en datalekken	Beleid datalekken KW1C	Eigen versie
15	Autorisatie en authenticatie	Autorisatie- en authenticatiebeleid KW1C	Eigen versie
16	Schooleigendommen meenemen buiten KW1C	Reglement verantwoord computergebruik	Eigen versie
17	Clear desk / clear screen	Clear desk/Screen policy	Eigen versie
18	Thuiswerken	Thuiswerkbeleid HR	Eigen versie

IMPLEMENTATIEPLAN
Intern moeten procedures en richtlijnen voortvloeiend uit dit beleid, communicatie, borging en evaluatie opnieuw opgesteld, overlegd en vastgelegd worden. De IBP-organisatie is hier leidend in.

VERVALLEN BELEID
Per 1 augustus 2023 komen de volgende documenten te vervallen:

- Informatie en privacy beleid, vastgesteld 14 december 2020 (Oud Leijgraaf)
- Informatiebeveiligingsbeleid KW1C, vastgesteld 01 september 2020 (Oud KW1C)

Per 1 oktober 2025 komen de volgende documenten te vervallen:

- Informatiebeveiligingsbeleid KW1C, vastgesteld 06 juni 2023