Informatiebeveiligings- en privacy beleid Isendoorn College - 1.5

Bron: **Kennisnet**

Bewerkt voor: **Het Isendoorn College**

Versie	Status	Datum	Auteur	Datum akkoord
1.5	Teksten gereed	Feb. 2022	HAF	
1.5	Beoordeeld door FG	08-03-2022		9 maart 2022
1.5	Ter instemming naar MR	22-03-2022		29 maart 2022
1.5	Ter bespreking naar MT	30-03-2022		5 april 2022

Vastgesteld door het Isendoorn College

Versie	Datum	Naam	Functie
1.5	05-04-2022	E.Lutteke	Rector/Bestuurder

Inhoudsopgave

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** (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.

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 schades 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 onder andere 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, verstrekken 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

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, verder te benoemen als IBP-beleid, vormt de basis om informatiebeveiliging en privacy binnen het Isendoorn College te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3 Doel en reikwijdte

3.1 Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

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

Het informatiebeveiligings- en privacy beleid (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 hun ouders/verzorgers) wordt gerespecteerd en het Isendoorn College voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen het Isendoorn College geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing)

- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen het Isendoorn College waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan het Isendoorn College persoonsgegevens verwerkt.

- Het beleid geldt voor alle toepassingen die vallen onder de verantwoordelijkheid van het Isendoorn College. 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 en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media).

- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van het Isendoorn College 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.

- IBP-beleid heeft binnen het Isendoorn College raakvlakken met:
  - *Algemeen (sociaal) veiligheidsbeleid;* met als aandachtspunten bedrijfshulpverlening, crisismanagement, huisvesting en ongevallen
  - *Personeels- 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, hun ouders/verzorgers en medewerkers

4 Beleid – Hoe doen we dat?

het Isendoorn College hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van het Isendoorn College neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld worden. 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 Isendoorn College voldoet aan alle relevante wet- en regelgeving.

3. Bij het Isendoorn College 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 Isendoorn College 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.

4. Het Isendoorn College informeert alle betrokkenen helder en actief over de verwerkingen van de 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, overdracht van de gegevens en profilering.

5. Het Isendoorn College legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Het Isendoorn College voldoet hiermee aan de documentatieplicht.

6. Binnen het Isendoorn College 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 van papieren documenten.

7. Het Isendoorn College 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.

8. Het Isendoorn College 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.

9. Het Isendoorn College 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.

10. Het Isendoorn College 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. Het Isendoorn College heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd. Deze is te vinden in het personeelsportaal.

11. Informatiebeveiliging en privacy is bij het Isendoorn College een continu proces, waarbij regelmatig wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. Het Isendoorn College 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. Indien noodzakelijk wordt er een Data Protectie Impact Assessment (DPIA). De uitkomst van de DPIA bepaalt de te nemen aanvullende maatregelen.

13. Het Isendoorn College 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.

14. Het Isendoorn College zal alle beveiligingsincidenten vastleggen en datalekken conform het stappenplan en advies van de functionaris gegevensbescherming afhandelen en zo nodig melden bij de Autoriteit Persoonsgegevens en aan de betrokkenen.

5 Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten.

5.1 Relevante wet- en regelgeving

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

- Wet op het voortgezet onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen. 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.

5.2 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 staan 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, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. 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.

5.3 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en/of protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft inzicht met betrekking tot deze aanvullingen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

5.4 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 IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP, de FG, en de Security Officer met het bestuur als eindverantwoordelijke.

5.5 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 (=BIV-classificatie). Deze classificatie is terug te vinden als onderdeel van het dataregister.
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.

5.6 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 het *Incidentenregister Datasecurity* dat wordt bijgehouden en bewaard bij het directiesecretariaat. Alle (beveiligings)incidenten moeten worden gemeld bij de privacy officer (conrector) en bij het directiesecretariaat (directie@isendoorn.nl).
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig zullen aanvullende passende beleidsmaatregelen genomen worden.

5.7 Planning en controle

Dit IBP-beleid wordt met enige regelmaat getoetst en bijgesteld door het MT. 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

5.8 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, door middel van een gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. Het Isendoorn College maakt gebruik van een onafhankelijke externe FG en heeft daartoe een contract afgesloten met *'Privacy op School'*. De FG is bereikbaar via fg@privacyopschool.nl.

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

5.9 Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt er voor 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.

6 Organisatie - Wie doet wat?

6.1 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 op het Isendoorn College.

Het MT, bestaande uit de rector/dagelijks bestuurder (eindverantwoordelijke), de conrector (in het kader van dit document tevens de privacy officer) en teamleiders formuleren het IBP-beleid en zien toe op de naleving ervan. De MR heeft instemmingsrecht op het IBP-beleidsplan.

De functionaris gegevensbescherming (FG) zorgt vanuit een onafhankelijke en externe positie voor toenemende bewustwording rondom IBP binnen de organisatie, begeleidt de afhandeling van informatiebeveiligingsincidenten, adviseert gevraagd en ongevraagd over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke. De FG heeft regelmatig overleg met de privacy officer. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen van binnen en buiten de organisatie.

Proceseigenaren zijn o.a. de systeembeheerders (ICT), de personeelsfunctionaris (HRM / P&O), de applicatiebeheerder SOM, het hoofd facilitaire dienst (tevens hoofd BHV en veiligheidscoördinator), de administratief medewerkers en de docenten. Zij zorgen in gezamenlijkheid en elk voor het eigen deel onder andere voor:

- een correcte toepassing van het toegangsbeleid zowel fysiek/analoog als digitaal en bewaken daarmee mede dat persoonsgegevens alleen bereikbaar, verwerkbaar en inzichtelijk zijn voor daartoe bevoegde medewerkers van de eigen organisatie of van bedrijven en instanties waarmee een verwerkersovereenkomst is afgesloten (bij twijfel: informeer bij de privacy officer).
- dat gebruikers alleen toegang hebben tot het netwerk, delen van het netwerk en netwerkdiensten waarvoor zij specifiek bevoegd zijn.
- dat de toegangsrechten van gebruikers correct zijn toegewezen en er geen misbruik wordt gemaakt.
- dat protocollen en overige afspraken in het kader van IBP-beleid worden nageleefd.

De privacy officer zorgt onder andere voor:

- Incidentafhandeling (registreren, communiceren met de FG en evalueren).
- Communicatie naar alle betrokkenen; er voor 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.
- periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- IBP-beleid actueel houden

7 Welke documenten zijn verbonden met het IBP?

Het IBP is geen alleenstaand document. Er zijn diverse andere beleidsstukken die in relatie staan met het IBP of die nadere invulling geven aan het IBP. Hieronder een opsomming:

Tevens onderdeel van het IBP zijn of worden:

- Het dataregister voor leerlingen *)
- Het dataregister voor personeel *)
- Het dataregister overige contacten *)

*) nog in opbouw

- Netwerkbeveiligingsplan Isendoorn College *"Netwerkveiligheid 2021"*

Daarnaast zijn op de website van het Isendoorn College de volgende documenten en protocollen te vinden die in directe relatie staan met het privacy- of beveiligingsbeleid van de school (zie het personeelsportaal en de online schoolgids):

- Cameratoezicht op school
- Gedragscode medewerkers Isendoorn College
- Gedragscode sociale media
- Geheimhoudingsverklaring externen
- Grenzen aan gedrag
- Handvatten voor het personeel m.b.t. privacyregels in het kader van de AVG
- Integriteitscode Isendoorn College
- Klachten regeling
- Klokkenluidersregeling Isendoorn College
- Leerlingenstatuut
- Pestprotocol

Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

Thema:	Toelichting:
Procedure toestemming gebruik beeldmateriaal	Ouders/leerlingen 16+ wordt gevraagd om toestemming via Somtoday. Zie voor resultaten: portretrecht in Somtoday.
Procedure voor verwijderen van gegevens	Bewaartermijnen zijn ingesteld conform regelgeving in Somtoday en YouForce. Opschoning gebeurt minimaal één keer per jaar.
Procesbeschrijving rechten betrokkenen	zie: document “Informatieplicht bij gescheiden ouders” in schoolgids
Privacyreglement	zie Privacy Policy in schoolgids
Autorisatiematrix	Iedereen heeft een rol met specifieke toegangsrechten tot de verschillende (onderdelen van de) systemen. Deze rollen zijn vastgelegd in die systemen (Somtoday, Zermelo YouForce, etc.)
Afspraken gebruik sociale media	zie mediaprotocol en overige protocollen in personeelsportaal.
Cameratoezicht	Beelden van beveiligingscamera’s worden uitsluitend uitgelezen door daartoe bevoegde werknemers. Indien de situatie daarom vraagt krijgen politie en justitie ook toegang tot deze beelden in het kader van het convenant veilige school (zie schoolgids).
Wachtwoordbeleid	Minimaal jaarlijks worden alle medewerkers gedwongen tot het kiezen van een nieuw sterk wachtwoord om in te kunnen loggen in de Isendoorn systemen. Inloggen kan alleen via tweefactor authenticatie.
Gedragscode ict en internetgebruik/personeel	1. zie personeelsportaal en paragraaf 7 hierboven 2. gebruikersovereenkomsten voor iPad en/of laptop van de school moeten worden ondertekend alvorens een device beschikbaar wordt gesteld. 3. bij indiensttreding c.q. start werkzaamheden wordt een geheimhoudingsverklaring ondertekend.
Gedragscode ict en internetgebruik/leerlingen	Zie diverse protocollen op de website via deze link: https://www.isendoorn.nl/praktische_info/protocollen
Procedure rondom uitwisselen gegevens	Uitwisselen met andere onderwijsinstellingen gaat via de beveiligde kanalen van OSO. Informatie in het kader van passend onderwijs, leerling dossiers, leerplicht, enz. worden uitgewisseld via een versleutelde route.

Verplicht vanuit de AVG:

Procesbeschrijving melden datalekken
Elk datalek of vermoeden daarvan moet gemeld worden bij de privacy officer. Deze zal vervolgens handelen volgens de stappen in bijlage 2.

Registratie beveiligingsincidenten
Van beveiligingsincidenten wordt registratie bijgehouden door de privacy officer van de school en bewaard in het archief van het directiesecretariaat. Deze registratie is op eerste verzoek in te zien door de rector/bestuurder, de FG, de accountant van de school en de Autoriteit Persoonsgegevens.

Dataregister om te voldoen aan de registratieplicht *)
Er is een dataregister voor leerlinggegevens, medewerkersgegevens en voor overige contacten. Een actuele kopie wordt opgeslagen bij het directiesecretariaat
**) nog in ontwerp*

Verwerkersovereenkomsten
Het Isendoorn College sluit een verwerkersovereenkomst af met elke externe partij die persoonsgegevens verwerkt namens het Isendoorn College. Een lijst van bedoelde partijen met de betreffende overeenkomst wordt bijgehouden door het directiesecretariaat van de school.

Procedure gegevensbeschermingseffectbeoordeling/Risicoanalyse/DPIA
De term Data Protection Impact Assessment (DPIA) wordt in het Nederlands gegevensbeschermingseffectbe-oordeling' genoemd. Het Isendoorn College Isendoorn kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy. Indien noodzakelijk wordt er een Data Protectie Impact Assessment (DPIA) uitgevoerd met advies van de FG. De uitkomst van de DPIA bepaalt de te nemen aanvullende maatregelen.

Functionaris voor Gegevensbescherming
Het Isendoorn College maakt gebruik van een onafhankelijke, contractueel aan de school verbonden extern deskundige FG. Deze handelt en adviseert conform de daarvoor geldende wettelijke regelgeving.

Bijlage 2: Stappenplan: wat te doen bij een datalek

Een datalek kan grote schade veroorzaken, zowel aan het imago en de continuïteit van de organisatie, maar in sommige gevallen ook aan de persoonlijke levenssfeer van de betrokkenen. Het is bij een dergelijk incident belangrijk adequaat te handelen. Dit stappenplan zal in voorkomende gevallen gebruikt worden als handleiding. In geval van een datalek of bij het minste vermoeden van een serieus datalek zal de FG vanaf het begin worden ingeschakeld om onderstaande stappen te begeleiden. Indien van toepassing kan op advies van de FG afgeweken worden van onderstaand stappenplan.

Stap 1: Stel vast of er daadwerkelijk sprake is van een datalek

Allereerst is het zaak om vast te stellen of een datalek daadwerkelijk heeft plaatsgevonden. Er is sprake van een datalek wanneer persoonsgegevens:

- al dan niet met opzet zijn gestolen of zijn kwijtgeraakt. Denk daarbij bijvoorbeeld aan verlies van een mobiele schijf of USB-drive met privacygevoelige data op straat of in de trein. Maar bijvoorbeeld ook persoonsgegevens die verloren gaan door brand is een datalek;
- op een onrechtmatige manier zijn verwerkt. Bijvoorbeeld wanneer gevoelige data is opgeslagen zonder medeweten of toestemming van de betrokkene;
- gegevens worden ingezien en/of bewerkt door niet-bevoegd personeel;
- data langer dan de afgesproken periode zijn bewaard, tenzij de betrokkene daar expliciet toestemming voor gegeven heeft;
- langer zijn bewaard dan nuttig voor het beoogde doel, tenzij de betrokkene daar expliciet toestemming voor gegeven heeft

Verlies, verwerking of diefstal van andere data dan persoonsgegevens zijn geen datalekken. Wanneer bijvoorbeeld broncode van door uw organisatie ontwikkelde software in handen komt van onbevoegd personeel of een hacker, dan spreken we niet van een datalek. Persoonsgegevens zijn altijd herleidbaar naar personen, denk aan inloggegevens, NAW-gegevens, creditcardgegevens, medische informatie, data over geslacht, politieke of seksuele voorkeur, persoonlijke financiële data of bijvoorbeeld BSN-nummers.

Stap 2: Neem maatregelen om een ‘actief’ lek te stoppen

In sommige gevallen is er sprake van een ‘actief’ datalek, bijvoorbeeld wanneer een hacker of onbevoegde medewerker mogelijk nog toegang tot de data heeft en nog altijd nieuwe gegevens kan buitmaken. Hackers blijven soms weken, maanden of zelfs jaren onopgemerkt in het netwerk en kunnen gedurende die tijd ongestoord data stelen. Het is dus cruciaal dat een aanval snel wordt gedetecteerd.

Maar ook medewerkers kunnen ongeoorloofd toegang hebben tot gegevens en zo een permanent datalek veroorzaken. In alle gevallen is het uiteraard zaak zo snel mogelijk te handelen en het gevaar te mitigeren. Bijvoorbeeld door het blokkeren van accounts, het verplaatsen van de data naar een veilige locatie of het isoleren van een indringer van buitenaf. Schakel professionele hulp in als het eigen team hier niet toe in staat blijkt.

Stap 3: Verzamel zoveel mogelijk informatie

Het is van groot belang om zoveel mogelijk informatie in te winnen over het datalek. Niet alleen over de aard van het lek zelf, zoals hoeveel en welke gegevens precies gelekt zijn, maar vooral ook wat daar precies aan vooraf ging en hoe het lek heeft kunnen plaatsvinden.

Op het Isendoorn zijn de IT-systemen zo ingericht dat deze informatie continu vanzelf verzameld wordt. Zo worden onder andere logbestanden met bestandswijzigingen en transfers bijgehouden, gekoppeld aan gebruikers. Dit geeft mogelijkheden om te achterhalen wie toegang heeft gehad tot bepaalde data en wat deze persoon daarmee deed.

Deze informatie is niet alleen waardevol voor de eigen organisatie, maar ook van groot belang bij eventueel noodzakelijk forensisch onderzoek. Bovendien kan een gedetailleerd rapport over het lek de kans verkleinen dat de organisaties volgens de Autoriteit Persoonsgegevens nalatig heeft gehandeld.

Stap 4: Meld het lek indien noodzakelijk bij de Autoriteit Persoonsgegevens (AP)

De AVG bepaalt dat datalekken direct, binnen 72 uur na de bekendwording, gemeld moeten worden aan de AP. tenzij het niet waarschijnlijk is dat de inbreuk met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van de betrokkenen. Bij de afweging of het datalek gemeld moet worden bij de AP weegt het advies van de FG zwaar.

Stap 5: Meld het lek indien noodzakelijk bij de betrokkenen

Volgens de AVG moet naast een melding bij de AP, het datalek ook aan de betrokkenen gemeld worden indien het lek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt. Dat zijn in dit geval de mensen wier gegevens zijn gelekt. Organisaties zijn dit verplicht wanneer een lek mogelijk schadelijk is voor de ‘persoonlijke levenssfeer’ van de betrokkenen. Schade is hier een breed begrip: het gaat om mogelijke schade aan bijvoorbeeld het imago, de privacy of financiële schade.
Bij de afweging of het datalek gemeld moet worden bij de betrokkenen weegt het advies van de FG zwaar.

Stap 6: Neem preventieve maatregelen om het lek in de toekomst te voorkomen

Na een datalek is het van groot belang er alles aan te doen een dergelijk incident in de toekomst te voorkomen. Het uitgevoerde onderzoek, de adviezen van de FG en adviezen van eventuele overige externe partijen moeten samen een goede evaluatie en vervolg acties opleveren die kunnen leiden tot voorkoming van herhaling.