Scholengemeenschap
Sint-Donaas
Magdalenastraat 30
8200 Brugge

INFORMATIEVEILIGHEIDS- EN PRIVACYBELEID

Vzw Secundair Onderwijs Karel de Goede

voor:

Sint-Jozef Humaniora

Inhoud

Deel 1 Algemeen deel

1.1 Inleiding

Onze scholen willen persoonsgegevens verwerken conform de wetgeving rond informatieveiligheid zoals gestipuleerd in de *Algemene Verordening Gegevensbescherming* of *General Data Protection Regulation* van 25 mei 2018. In deze tekst verwoordt Sint-Jozef Humaniora hoe zij daar beleidsmatig mee omgaat.

1.1.1 Toelichting informatieveiligheid

Onder informatieveiligheid wordt verstaan: het nemen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de verwerking van persoonsgegevens zo maximaal mogelijk te garanderen.

Deze kwaliteitsaspecten zijn:

- **Beschikbaarheid:** de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- **Integriteit:** de mate waarin gegevens en/of functionaliteiten juist, volledig en actueel zijn.
- **Vertrouwelijkheid:** de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot zij die daartoe bevoegd zijn.
- **Controleerbaarheid:** de mate waarin het mogelijk is om achteraf parameters die van belang zijn voor beschikbaarheid, integriteit of vertrouwelijkheid te verifiëren.

Onvoldoende informatieveiligheid kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en bij de dagdagelijkse werking van de onderwijsinstelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imagoverlies.

1.1.2 Toelichting *privacy*

Privacy gaat over de manier waarop persoonsgegevens beschermd worden conform de huidige wet- en regelgeving. De bescherming van de *privacy* regelt onder andere de voorwaarden waaronder persoonsgegevens gebruikt mogen worden, maar is ook gelinkt aan de camerawet.

Persoonsgegevens zijn hierbij alle gegevens van een geïdentificeerd of identificeerbaar individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. Denken we maar aan het verzamelen, raadplegen, bijwerken, verspreiden tot en met het wissen van deze gegevens.

1.1.3 Vervlechting informatieveiligheid en *privacy*

Informatieveiligheid is noodzakelijk om *privacy* te waarborgen. Beide begrippen zijn met elkaar verbonden. Het onderwerp informatieveiligheid en *privacy* wordt afgekort tot IVP. Deze beleidstekst ligt ten grondslag aan de aanpak van informatieveiligheid en *privacy* binnen Sint-Jozef Humaniora.

1.2 Doel en reikwijdte

1.2.1 Doel

Dit beleid heeft als doel:

- Het waarborgen van de continuïteit van de onderwijsorganisatie en de dagdagelijkse werking van Sint-Jozef Humaniora.

- Het garanderen van de *privacy* van leerlingen, personeelsleden, onderwijspartners en derden waardoor beveiligings- en *privacy*-incidenten zoveel mogelijk worden voorkomen.

- De kwaliteit van de verwerking van persoonsgegevens te optimaliseren.

1.2.2 Reikwijdte

- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Sint-Jozef Humaniora.

- Dit beleid is van toepassing op zowel de digitale als geschreven verwerking van persoonsgegevens.

- Het IVP-beleid geldt voor alle personeelsleden, leerlingen, onderwijspartners en derden die binnen een professionele context persoonsgegevens verwerken.

- Het beleid heeft betrekking op gecontroleerde informatie die door onszelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en sociale media. Hiervoor werkt Sint-Jozef Humaniora met **gedragscodes** zoals uitgewerkt binnen het communicatiebeleid (zie onderdeel 'IVP-communicatiebeleid').

- Het IVP-beleid binnen Sint-Jozef Humaniora heeft raakvlakken met:
  - het algemeen preventie- en welzijnsbeleid en toegangsbeveiligingsbeleid, met als voorbeelden EHBO-verlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen;
  - het personeels- en organisatiebeleid, met als voorbeelden de in- en uitstroom van personeelsleden, functiewisselingen, functiescheiding en vertrouwensfuncties;
  - het IT-beleid, met als voorbeelden de aanschaf, het beheer, het gebruik en/of het uit dienst stellen van hardware, software, services en (digitale) leermiddelen;
  - Het participatiebeleid van leerlingen, ouders en personeelsleden.

1.3 Uitgangspunten

1.3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij Sint-Jozef Humaniora zijn:

- IVP dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de **Algemene Verordening Gegevensbescherming** (AVG). De verwerking van persoonsgegevens is steeds gebaseerd op één van de in deze verordening vastgelegde rechtmatigheden (zie verder) waarbij het uitgangspunt is dat de persoonlijke levenssfeer van alle betrokkenen wordt gerespecteerd.

- Het schoolbestuur, vzw Secundair Onderwijs Karel de Goede, is als rechtspersoon de **verwerkingsverantwoordelijke** voor alle persoonsgegevens die in opdracht van Sint-Jozef Humaniora verwerkt worden.

- Sint-Jozef Humaniora beheert ook informatie waarvan de intellectuele eigendom (het **auteursrecht**) toebehoort aan derden. Personeelsleden en leerlingen moeten dus goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.

- De waarde van deze informatie kan door Sint-Jozef Humaniora geclassificeerd worden waarbij het beleid een balans maakt tussen de risico's van hetgeen we willen beschermen en de benodigde maatregelen.

- Sint-Jozef Humaniora sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) **verwerkersovereenkomsten** af indien deze persoonsgegevens ontvangen van de school.

- Binnen Sint-Jozef Humaniora 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 fysieke documenten.

- Er wordt van alle personeelsleden, leerlingen, onderwijspartners en derden verwacht dat zij zich verantwoordelijk gedragen.

- Bij wijzigingen in de infrastructuur, de aanschaf en de uit dienst name van (informatie)systemen, wordt bij Sint-Jozef Humaniora steeds rekening gehouden met IVP.

- IVP is bij Sint-Jozef Humaniora een continu proces, waarbij regelmatig (minimaal driejaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

1.3.2 Uitgangspunten *privacy*

De zes vuistregels met betrekking tot het omgaan met persoonsgegevens bij Sint-Jozef Humaniora zijn:

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 verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op één van de wettelijke rechtmatigheden: toestemming, overeenkomst, wettelijke verplichting, openbaar belang, vitaal belang van de betrokkene of gerechtvaardigd belang.
3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken. Ze staan in verhouding tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt.
4. **Transparantie**: Sint-Jozef Humaniora legt aan alle betrokkenen op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IVP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op inzage, verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Opslagbeperking:** data wordt niet langer bewaard dan noodzakelijk. De verwerking wordt door het IVP-beleid beperkt in de tijd.
6. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn, en dat zij voldoende beschikbaar zijn om de werking van Sint-Jozef Humaniora te waarborgen. Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van **toestemming**, zal Sint-Jozef Humaniora een eenduidige procedure hanteren die een actieve en aantoonbare handeling vereist.

1.4 Organisatie

De organisatie van IVP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Dit hoofdstuk beschrijft hoe IVP in Sint-Jozef Humaniora is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Voor elk niveau wordt beschreven welke verantwoordelijkheden en taken de verschillende rollen met zich meebrengen.

1.4.1 Richtinggevend

Verwerkingsverantwoordelijke

Het schoolbestuur is eindverantwoordelijk voor IVP en stelt het beleid en de basismaatregelen op het gebied van IVP vast.

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

Zie bijlage 1 voor een schematische weergave van de rol- en taakverdelingen aangaande IVP op Sint-Jozef Humaniora en binnen S.O. Karel de Goede vzw.

1.4.2 Sturend

***Data Protection Officer* (DPO) van de koepelorganisatie**

Vanuit de koepelorganisatie Katholiek Onderwijs Vlaanderen wordt er een *Data Protection Officer* aangesteld. Deze zal binnen het schoolbestuur of instelling het Aanspreekpunt Informatieveiligheid (AIV) aansturen. De taak bestaat uit:

- schoolbesturen informeren en adviseren over hun verplichtingen vanuit de AVG en vanuit andere gegevensbeschermingsbepalingen;
- AIV's opleiden en hulpmiddelen verstrekken zodanig dat ze binnen hun instelling(en) het IVP-beleid kunnen ondersteunen;
- desgevraagd advies verstrekken over de gegevensbeschermingseffectbeoordeling;
- met de toezichthoudende autoriteit samenwerken en optreden als aanspreekpunt voor deze autoriteit.

Aanspreekpunt Informatieveiligheid

Het AIV is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (directie van de instelling, raad van bestuur van het schoolbestuur) en staat de mensen op uitvoerend niveau bij. Het AIV moet:

- het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling;
- de uniformiteit bewaken binnen Sint-Jozef Humaniora;
- meewerken aan de bewustmaking en opleiding van het personeel;
- het aanspreekpunt zijn voor incidenten op het gebied van IVP;
- de verdere afhandeling van incidenten binnen Sint-Jozef Humaniora coördineren.

1.4.3 Uitvoerend

Leidinggevende

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

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid;
- toe te zien op de naleving van het IVP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IVP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeelgerelateerde IVP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door het AIV.

ICT-coördinator

De ICT-coördinator vormt een technisch aanspreekpunt inzake informatieveiligheid voor het management en de medewerkers, en zorgt in de praktijk voor de implementatie van toegangsrechten en de rapportage aangaande digitale informatieveiligheid.

Personeelslid

Alle personeelsleden hebben een verantwoordelijkheid met betrekking tot informatieveiligheid in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in alle IVP-teksten.

Personeelsleden zijn actief betrokken bij informatieveiligheid. Dit gebeurt door meldingen te maken van veiligheidsincidenten, het doen van voorstellen ter verbetering van IVP en het uitoefenen van invloed op het beleid (individueel of via de ervoor voorziene overlegorganen en/of via het aanspreekpunt). Zelf hebben zij ook een voorbeeldfunctie naar andere personeelsleden, externen en vooral leerlingen toe.

Van ambtswege uit, of eventueel contractueel, worden alle personeelsleden en derden van Sint-Jozef Humaniora die toegang kunnen hebben tot persoonsgegevens, gebonden aan een discretieplicht. Welbepaalde (externe) medewerkers zijn wettelijk gebonden aan een beroepsgeheim.

1.5 Controle en rapportage

Dit IVP-beleid en alle bijhorende richtlijnen, nota's en tools, worden minimaal elke twee jaar getoetst en bijgesteld door het schoolbestuur. Hierbij wordt rekening gehouden met:

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

Daarnaast kent Sint-Jozef Humaniora minimaal driejaarlijks een planning en controlecyclus voor IVP. Dit is een vast evaluatieproces waarmee de inhoud en effectiviteit van het IVP-beleid wordt getoetst.

Het resultaat van deze rapportage en controle wordt best opgenomen in bestaande overlegvormen:

- **strategisch** niveau (richtinggevend) wordt gesproken over organisatie, alsmede over doelen, bereik en ambitie op het gebied van IVP;
- **tactisch** niveau (sturend) de strategie wordt vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering;
- **operationeel** niveau (uitvoerend) de onderwerpen worden besproken die de dagelijkse uitvoering aangaan. Deze overlegvorm wordt niet centraal georganiseerd, en indien nodig in elk organisatieonderdeel van Sint-Jozef Humaniora afzonderlijk.

1.5.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatieveiligheid en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij Sint-Jozef Humaniora 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 onder andere de regelmatig terugkerende bewustwordingscampagnes voor iedereen binnen de school. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van het AIV en leidinggevende(n), met de Raad van bestuur van S.O. Karel de Goede vzw als eindverantwoordelijke.

1.5.2 Incidenten en datalekken

Bij Sint-Jozef Humaniora is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

Alle incidenten kunnen worden gemeld bij privacy@sintjozefhumaniora.be. De afhandeling van deze incidenten volgt een gestructureerd proces, waarbij men ook voorziet in de juiste stappen rondom de meldplicht datalekken.

1.5.3 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IVP-proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij Sint-Jozef Humaniora wordt actief aandacht besteed aan IVP bij de inschrijving van leerlingen, de indiensttreding van personeelsleden, tijdens periodieke bewustwordingscampagnes, enzovoort.

Mocht de naleving ernstig tekort schieten, dan kan Sint-Jozef Humaniora de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden. Voor de bevordering van de naleving van de AVG heeft het AIV een belangrijke rol.

Bijlagen bij deel 1:

Bijlage 1: Tabel IVP-rollen en -taken

Wie **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
School- of centrumbestuur S.O. Karel-de-Goede	● Eindverantwoordelijke ● IVP-beleidsvorming, -vastlegging en het uitdragen ervan ● Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens ● Evalueren toepassing en werking IVP-beleid op basis van rapportages en bijsturen van dit beleid indien nodig ● Organisatie IVP inrichten	● Informatieveiligheids- en privacy beleid opstellen en goedkeuren en communiceren ● Aanspreekpunt informatieveiligheid aanstellen ● Oprichten veiligheidscel
Leidinggevende (directie) D. Maes S. Lecomte	● Toezien op de naleving van het IVP-beleid en privacywetgeving en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. ● Communicatie naar alle betrokkenen; er voor zorgen dat alle medewerkers op de hoogte zijn van het IVP-beleid en de consequenties ervan. ● Voorbeeldfunctie met positieve en actieve houding t.a.v. IVP-beleid. ● Rapporteren voortgang m.b.t. doelstellingen IVP-beleid aan bestuur ● Periodiek het onderwerp informatiebeveiliging onder de aandacht brengen in werkoverleg, beoordelingen,… ● Implementeren IVP-maatregelen.	Communiceren, informeren en toezien op naleving van o.a.: ● IVP in het algemeen ● Hoe omgaan met leerlingendossiers ● Wie mag wat zien ● Gedragscode ● Beveiliging van ruimtes ● Preventieve maatregelen (o.a. brand en waterschade aan servers…) ● …
Data protection officer koepel Gino De Meester	● Schoolbesturen informeren en adviseren over hun verplichtingen krachtens de AVG en regelgeving; ● Richtlijnen, kaders, procedures opstellen en aanbevelingen doen m.b.t. informatieveiligheid en privacy ● Aanspreekpunten IVP opleiden en hen de nodige tools en hulpmiddelen verstrekken ● desgevraagd advies verstrekken over de gegevensbeschermingseffectbeoordeling ● samenwerken met de toezichthoudende autoriteit en optreden als aanspreekpunt voor deze autoriteit ● Brugfiguur naar de externe partijen toe ● Lerend netwerk ontwikkelen en aansturen	● Opstellen van algemene processen, richtlijnen en sjablonen IVP ● Nascholingstraject organiseren ● Overleg met informatieveiligheidsconsulenten onderwijsnetten en GO! ● Overleg met externe partijen: leveranciers van leerlingadministratie en -volgsysytemen en leveranciers van didactische software ● Tools aanpassen/ontwikkelen

Wie **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
Aanspreekpunt informatieveiligheid Soetkin Smets	● Informeert en adviseert directie/bestuur en personeel over IVP ● Rapporteert naar directie/bestuur ● Informeert de data protection officer van de koepel ● Meewerken aan de uitwerking van een specifiek IVP-beleid op basis van het algemeen IVP-beleid ● Voorstellen doen tot aanpassingen van centraal aangeboden processen, richtlijnen en procedures om de uitvoering van het IVP-beleid te ondersteunen binnen de school ● Meewerken aan: o classificatie van middelen o risicoanalyse o het opstellen van een veiligheidsplan ● Aanspreekpunt voor IVP-incidenten ● Incidentafhandeling (registreren en evalueren). ● Invullen register verwerkingsactiviteiten	Voorstellen van aanpassingen aan de uitgewerkte formulieren van processen, richtlijnen en procedures rond IVP, bijvoorbeeld: ● Security awareness activiteiten ● Authenticatie en autorisatie-beleid ● Gedragscodes (ICT en internetgebruik, sociale media, privacybeleid…) naar medewerkers en leerlingen toe ● Verwerkersovereenkomsten regelen ● Toestemming opstellen gebruik foto's en video ● Communicatieplan naar medewerkers, leerlingen, ouders en cursisten ● Procedure IVP-incident afhandeling ● Inrichten meldpunt datalekken ● Melden datalekken naar de overheid toe ● … Invullen van register verwerkingsactiviteiten voor schooleigen situatie
Informatieveiligheidscel (CIV) van de school of het schoolbestuur [1] D. Maes S. Lecomte S. Smets B. Blondeel I. Ryheul	● Classificatie van informatie ● IVP risicoanalyse uitvoeren ● Prioriteiten voorstellen ● Toegangsbeleid zowel fysiek als digitaal vaststellen en laten bekrachtigen door bestuur ● De toegangsrechten van gebruikers regelmatig beoordelen en controleren. ● Evalueren IVP-beleid en voorstellen van verbetermaatregelen ● Bespreking veiligheidsincidenten en voorstellen formuleren voor te nemen maatregelen ● Aanpassen gegevensbeschermings-effectbeoordeling aan eigen situatie	● Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) ● Classificatie van informatiebronnen en persoonsgegevens ● Risicoanalyse uitvoeren en documenteren Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: ● Toegangsmatrix diverse informatiesystemen en netwerk
Iedereen	● Uitvoeren taken conform gegeven richtlijnen en procedures. ● Verantwoordelijk omgaan met IVP bij de dagelijkse werkzaamheden	Richtlijnen en procedures volgen Melden incidenten aan aanspreekpunt informatieveiligheid

[1] bestaande uit domeinverantwoordelijke/ proceseigenaren waaronder: ICT, personeelsdienst, preventieadviseur, financiën, leerlingenadministratie, facilitair management, leidinggevende en het aanspreekpunt informatieveiligheid

Deel 2 IVP-communicatiebeleid

2.1 Inleiding

De manier waarop alle betrokkenen communiceren maakt ook een deel uit van het IVP-beleid. In dit document worden enkele principes vastgelegd inzake interne én externe communicatie, om er samen voor te zorgen dat de privacy, de informatieveiligheid op en het imago van Sint-Jozef Humaniora bewaakt wordt.
Deze nota valt onder de eindverantwoordelijkheid van S.O. Karel de Goede vzw.

2.2 Gedragscodes

2.2.1 Gedragscode voor personeelsleden

1) Discretieplicht

Alle personeelsleden van Sint-Jozef Humaniora zijn gebonden aan een discretieplicht, ten aanzien van de persoonsgegevens van andere personeelsleden en van alle leerlingen, onderwijspartners en derden, conform artikel 23 van het *Algemeen reglement van het personeel van het katholiek onderwijs*.

Dit betekent dat personeelsleden van ambtswege uit, geen persoonsinformatie mogen vermelden of publiceren, buiten de daarvoor voorziene kanalen binnen Sint-Jozef Humaniora. Onderling informatie delen is enkel toegestaan via de hieronder vastgelegde kanalen en procedures, en steeds als dit in het belang is van de leerling of een collega in kwestie.

Personeelsleden worden van ambtswege uit geacht om de geldende IVP-procedures en IVP-afspraken steeds te volgen, teneinde het accidenteel verspreiden van persoonsgegevens te vermijden.

Als men vermoedt dat, door toedoen van uzelf of van anderen, er mogelijks persoonsgegevens buiten de context van deze discretieplicht verspreid werden, dan dient men het aanspreekpunt informatieveiligheid en/of het meldpunt datalekken hierover te contacteren. Voor Sint-Jozef Humaniora is het meldpunt datalekken: *privacy@sintjozefhumaniora.be*.

2) E-mail- en berichtenbeleid

Voor alle personeelsleden gelden de gedragscodes conform bijlage 3, punt 3.5 van het *Algemeen model van arbeidsreglement, opgesteld door Katholiek Onderwijs Vlaanderen*. Daarnaast leggen we richtlijnen vast inzake het doel, het gebruik en de beveiliging van de accounts. We maken een onderscheid tussen:

- (Algemeen-) Functionele mailaccounts van de school

Het e-mailbeheer van functionele schoolaccounts van het type sjh@sintjozefhumaniora.be, directie@sintjozefhumaniora.be, onthaal@sintjozefhumaniora.be, moneysafe@sintjozefhumaniora.be, … is toegewezen aan één of meerdere personeelsleden. Deze adressen worden vrij verspreid en gepubliceerd.

- Privémailadressen

Privéaccounts van het type voornaam.familienaam@hotmail.com, voornaam.familienaam@gmail.com, … worden niet gebruikt voor schoolgerelateerde communicatie met collega's, leerlingen, oud-leerlingen, ouders of externen.

Let op bij het gebruik van privéaccounts op toestellen waarop zich ook persoonsgegevens van Sint-Jozef Humaniora bevinden: dit kan risico's inhouden (virussen, randsomware, …).

- Individuele schoolaccounts

Deze accounts van het type voornaam.familienaam@sintjozefhumaniora.be worden toegewezen aan individuele personeelsleden voor professioneel gebruik. Het gebruik is dus verbonden met de taken die voortvloeien uit de functie. Deze adressen kunnen verspreid en gepubliceerd worden.
Gebruik deze accounts voor schoolgerelateerde externe communicatie met derden (b.v. stageplaatsen, de scholengemeenschap, …). Communicatie met collega's, leerlingen en ouders kan best gebeuren via het intern berichtensysteem (b.v. *Smartschool*).

- Berichtensystemen

Personeelsleden die gebruik maken van een berichtensysteem via communicatie-apps zorgen voor een maximale beveiliging (zie toestelbeleid).
Het interne berichtensysteem (b.v. *Smartschool*) is een gesloten communicatieplatform waarin wel persoonsgegevens gecommuniceerd kunnen worden.
Via externe berichtensystemen (*instant messaging, video conferencing*, …) worden geen persoonsgegevens gecommuniceerd.

3) *Social media*-protocol

Sociale media bieden een mogelijkheid om te laten zien dat men trots is op de school en kunnen een bijdrage leveren aan een positief imago van de school. Personeelsleden houden zich eraan om de goede naam van de school via sociale media niet te schaden en er verantwoord mee om te gaan, volgens de reguliere fatsoensnormen en in het verlengde van de missie en visie van de school.

Leerkrachten kunnen verantwoord gebruik maken van sociale media in de lespraktijk zolang dit past binnen een pedagogisch-didactische context.

Personeelsleden kunnen informatie en kennis delen, zolang deze niet vertrouwelijk of schadelijk is ten aanzien van anderen en zijn zelf verantwoordelijk voor de gepubliceerde inhoud.

Personeelsleden zijn er zich van bewust dat gepubliceerde informatie voor onbepaalde tijd openbaar blijft, ook na verwijdering van het bericht; en dat het publiceren van foto-, film- of geluidsopnames van schoolgerelateerde situaties op sociale media afhankelijk is van uitdrukkelijk toestemming.

2.2.2 Gedragscode voor leerlingen

1) Leefregels

Zie schoolreglement / ICT-protocol

2) E-mail- en berichtenbeleid

Leerlingen die gebruik maken van berichtensystemen via communicatie-apps (het schoolcommunicatieplatform, *instant messaging* via telefonie of *online, video conferencing*, enz.), doen dit conform de afspraken van het schoolreglement.

3) *Social media*-protocol

Leerlingen die gebruik maken van sociale media, gebruiken deze kanalen conform de afspraken van het schoolreglement.

2.2.3 Gedragscode voor derden

1) Discretieplicht

Derden die via hun dienst, levering of werk persoonsgegevens verwerken van personeelsleden, leerlingen of onderwijspartners sluiten een verwerkersovereenkomst af met de school.

2) *Social media*-protocol

Derden mogen binnen de schoolinfrastructuur geen foto-, film- of geluidsopnames maken van schoolgerelateerde situaties zonder uitdrukkelijke toestemming van de school. Het is niet toegelaten sociale media in de school te gebruiken die een goed en veilig schoolklimaat in het gedrang brengen.

2.3 *Privacy*-verklaringen

2.3.1 *Privacy*-verklaring voor personeelsleden

Zie bijlage 2

1) De wettelijke grondslag

Personeelsgegevens worden verwerkt door Sint-Jozef Humaniora / S.O. Karel de Goede vzw volgens regels vastgelegd in de *Algemene Verordening Gegevensbescherming* (AVG). Deze regelgeving beschermt personeelsleden bij de verwerking van gegevens, *in concreto* door de toepassing ervan door de personeelsadministratie van de school of het schoolbestuur en door passende beveiligingsmaatregelen tegen ongeoorloofde verwerkingen.

2) Uw persoonsgegevens

De personeelsadministratie van S.O. Karel de Goede vzw houdt zich eraan de persoonsgegevens op een bewuste, discrete, veilige en verantwoorde manier te verwerken. S.O. Karel de Goede vzw houdt een register bij van de manier waarop de persoonsgegevens verwerkt worden. Dit register brengt in kaart van wie en welke persoonsgegevens verwerkt worden, waarom dit gebeurt, door wie ze worden gedeeld, en voor welke termijn ze bewaard worden.

3) Recht op toegang

Personeelsleden kunnen persoonsgegevens die voor hem/haar van toepassing zijn in een gestructureerde elektronische vorm verkrijgen via de personeelsadministratie.

4) Recht op correctie en uitwissing

Personeelsleden kunnen de personeelsadministratie contacteren en hebben het recht op correctie als gegevens niet meer juist zijn, of uitwissing in het geval van toestemming. Personeelsleden hebben tevens meldingsplicht als personeelsadministratieve gegevens gewijzigd moeten worden.

5) Datalek

Als personeelsleden vermoeden dat persoonsgegevens buiten de context van deze discretieplicht verspreid werden, dan dient men het aanspreekpunt informatieveiligheid en/of het meldpunt datalekken hierover te contacteren. Voor Sint-Jozef Humaniora is het meldpunt datalekken: *privacy@sintjozefhumaniora.be*.

2.3.2 *Privacy*-verklaring voor leerlingen

Zie bijlage 1

1) De wettelijke grondslag

Leerlingengegevens worden verwerkt door Sint-Jozef Humaniora volgens regels vastgelegd in de *Algemene Verordening Gegevensbescherming* (AVG). Deze regelgeving beschermt leerlingen bij de verwerking van hun gegevens, *in concreto* door de toepassing ervan door de leerlingenadministratie van de school en door passende beveiligingsmaatregelen tegen ongeoorloofde verwerkingen.

2) Uw persoonsgegevens

De leerlingenadministratie van de school houdt zich eraan persoonsgegevens op een bewuste, discrete, veilige en verantwoorde manier te verwerken. Sint-Jozef Humaniora houdt een register bij van de manier waarop de persoonsgegevens verwerkt worden. Dit register brengt in kaart van wie en welke persoonsgegevens verwerkt worden, waarom dit gebeurt en door wie ze worden gedeeld, en hoe lang ze bewaard worden.

3) Recht op toegang

Leerlingen/ouders kunnen persoonsgegevens die voor hem/haar van toepassing zijn in een gestructureerde elektronische vorm verkrijgen.

4) Recht op correctie en uitwissing

Leerlingen/ouders kunnen de leerlingenadministratie contacteren en hebben het recht op correctie als gegevens niet meer juist zijn, of uitwissing in het geval van toestemming. Leerlingen/ouders hebben ook de plicht om relevante wijzigingen te melden aan de leerlingenadministratie.

2.3.3 *Privacy*-verklaring voor derden

1) De wettelijke grondslag

Gegevens van derden worden verwerkt door Sint-Jozef Humaniora volgens regels vastgelegd in de *Algemene Verordening Gegevensbescherming* (AVG). Deze regelgeving beschermt derden bij de verwerking van hun gegevens, *in concreto* door de toepassing ervan door de schooladministratie en door passende beveiligingsmaatregelen tegen ongeoorloofde verwerkingen.

2) Uw persoonsgegevens

De schooladministratie houdt zich eraan persoonsgegevens op een bewuste, discrete, veilige en verantwoorde manier te verwerken. Sint-Jozef Humaniora houdt een register bij van de manier waarop de persoonsgegevens verwerkt worden. Het register brengt in kaart van wie en welke persoonsgegevens verwerkt worden, waarom dit gebeurt en door wie ze worden gedeeld, en hoe lang ze bewaard worden.

3) Recht op toegang

Derden kunnen persoonsgegevens die voor hem/haar van toepassing zijn in een gestructureerde elektronische vorm verkrijgen.

4) Recht op correctie en uitwissing

Derden kunnen de schooladministratie contacteren en hebben het recht op correctie als gegevens niet meer juist zijn, of uitwissing in het geval van toestemming.

Bijlagen bij deel 2:

Bijlage 1: Privacyverklaring voor de leerling en zijn ouders

Privacyverklaring (leerling) – Sint-Jozef Humaniora

Wegens de wetgeving inzake informatieveiligheid en privacy, willen wij u informeren over de verwerkingen die wij met uw persoonsgegevens uitvoeren, en de beleidsmaatregelen die wij nemen om deze te beschermen.

1 Verantwoordelijken

Het schoolbestuur, S.O. Karel-de-Goede vzw, is de verwerkingsverantwoordelijke voor alle leerlingengegevens. Op Sint-Jozef Humaniora is er een aanspreekpunt informatieveiligheid aangeduid, dat gemakkelijk te contacteren is via privacy@sintjozefhumaniora.be. Het aanspreekpunt informatieveiligheid en/of de directie van Sint-Jozef Humaniora kan voor advies en ondersteuning terecht bij de 'data protection officer' (DPO) van de onderwijskoepel.

2 Verwerkingen

2.1 Verwerkingsdoeleinden

Op Sint-Jozef Humaniora verwerken wij leerlingengegevens omwille van de volgende doelen:

- leerlingenrekrutering;
- leerlingenadministratie;
- leerlingenbegeleiding;
- leerlingenevaluatie;
- public relations;
- toezicht op telecommunicatie;
- camerabewaking.

2.2 Verwerkte leerlingengegevens

Om u in te schrijven, te begeleiden en op te volgen in Sint-Jozef Humaniora is het noodzakelijk dat wij de volgende gegevens verwerken:

- identificatiegegevens (met in het bijzonder *voornaam en naam, roepnaam, een pasfoto, het rijksregisternummer, gezinssamenstelling, voorrang- en indicatorfactoren*);
- persoonlijke kenmerken (in concreto *geboortedatum, geboorteplaats, geslacht, nationaliteit*);
- privé contactgegevens (met i.h.b. *telefoonnummer(s), adresgegevens, e-mail*);
- evaluatiegegevens (met i.h.b. *puntenboeken, remediëring, rapporten, rapportcommentaren*);
- gezondheidsgegevens: *lichamelijk, psychisch, risicosituaties en -gedragingen (met het oog op begeleiding);*
- opleiding en vorming (met i.h.b. *vorige scholen, gevolgde richtingen, attesten, deliberatie-beslissingen, -motivaties en -verslagen, getuigschriften en diploma's*);
- aanwezigheid en discipline (met i.h.b. *afwezigheidsbewijzen, sancties, tucht*);
- afbeeldingen (*die niet administratief gebruikt worden*);
- bewakingsbeelden.

Deze gegevens kunnen, mits wettelijke grondslag, eventueel bekomen worden van de vorige school waar de leerling ingeschreven was.

2.3 Verwerkte oudergegevens

Om uw kind in te schrijven, te begeleiden en op te volgen in Sint-Jozef Humaniora is het noodzakelijk dat wij de volgende gegevens verwerken:

- elementaire identificatiegegevens;
- gezinssamenstelling;
- privé contactgegevens (met i.h.b. *telefoonnummer(s), adresgegevens, email*);
- financiële bijzonderheden (met i.h.b. *rekeningnummer, schoolonkosten, betalingen*).

2.4 Ontvangers

- Het departement onderwijs is, via het *Discimus*-systeem van AgODi, een ontvanger van een deel van jouw leerlingengegevens;
- de scholengemeenschap Sint-Donaas Brugge ontvangt uw administratieve gegevens omwille van hun bevoegdheden om onderwijssubsidies en -werkingsmiddelen te beheren;
- het CLB is, indien het jou begeleidt, bevoegd om alle in § 2.2 en § 2.3 opgesomde gegevens op te vragen;
- het ondersteuningsnetwerk is, indien van toepassing, bevoegd om een deel van de in § 2.2 en § 2.3 opgesomde gegevens op te vragen;
- iedereen die deel uitmaakt van het multidisciplinair team dat jou begeleidt, is bevoegd om alle in § 2.2 en § 2.3 opgesomde gegevens op te vragen;
- elke internaatsopvoeder die jou begeleidt, is bevoegd om een deel van de in § 2.2 en § 2.3 opgesomde gegevens op te vragen;
- bij verificatie krijgt de onderwijsverificateur toegang tot administratieve gegevens, aanwezigheden, afwezigheidsbewijzen, … in het kader van zijn wettelijk bepaalde taak;
- bij inspectie is het mogelijk dat een onderwijsinspecteur ook toegang vraagt tot bepaalde leerlingengegevens in het kader van zijn wettelijk bepaalde taak;
- hogescholen en universiteiten zijn ontvangers van een deel van jouw leerlingengegevens;
- hotels of jeugdherbergen zijn ontvangers van een deel van jouw persoonsgegevens bij excursies en reizen.

2.5 Verwerkers

Op Sint-Jozef Humaniora worden onderstaande platformen gebruikt bij de verwerking van leerlingengegevens:

- Informat
- Smartschool
- Integreat
- MoneySafe
- Google (Apps for Education en Drive)

2.6 Voorwaarden

Jouw gegevens zullen verwerkt worden zolang je bij ons ingeschreven bent, of zolang ze nodig zijn om je te begeleiden. Daarna worden ze verwijderd, geanonimiseerd of gearchiveerd conform de geldende regelgevingen.
Indien we bepaalde gegevens langer zouden willen bewaren, dan zullen we dat melden en de expliciete toestemming ervoor vragen.

Meer informatie over de beleidsmatige aanpak inzake privacy en informatieveiligheid op Sint-Jozef Humaniora kan je raadplegen op www.sintjozefhumaniora.be of opvragen via: privacy@sintjozefhumaniora.be.

3 Rechten inzake privacy

3.1 Rechten uitoefenen

U kan zich steeds op onderstaande rechten beroepen:
- recht op informatie: *u mag vragen welke gegevens van u er verwerkt worden en wie er toegang toe heeft (zie ook verwijzing in § 2.6), waarom de school die persoonsgegevens nodig heeft of gebruikt en hoe lang ze bewaard worden*;
- recht op inzage: *u mag steeds de gegevens die de school van u heeft, inkijken a.d.h.v. een kopie*;
- recht op verbetering: *als u fouten in uw gegevens vindt, mag u vragen om dit aan te passen. U kan ook aanvullingen toevoegen aan uw gegevens*;
- recht op gegevenswissing: *u kan vragen dat gegevens, die niet (meer) strikt noodzakelijk zijn voor de school, permanent en volledig verwijderd worden*;
- recht op beperking van de verwerking: *als u bezwaar hebt (zie verder) tegen de verwerking van bepaalde gegevens, kan u vragen om deze verwerking te stoppen*;
- recht op overdraagbaarheid van gegevens: *als u bepaalde gegevens wenst over te dragen naar een nieuwe school of andere werkgever, dan faciliteert de school dit (in de mate van het mogelijke)*;
- recht van bezwaar: *als u niet akkoord gaat met de grondslag van een verwerking of met de manier waarop bepaalde gegevens van u verwerkt worden, kan u zich hiertegen verzetten*;
- recht om niet te worden onderworpen aan geautomatiseerde besluitvorming: *wanneer de school algoritmes gebruikt om, zonder tussenkomst van mensen, bepaalde gevolgen te trekken uit (een deel van) uw gegevens (zie § 3.3), dan kan u zich hiertegen verzetten*;
- recht om zijn/haar toestemming in te trekken: *als men u voor bepaalde verwerkingen de toestemming gevraagd heeft, kan u ten allen tijde kiezen om deze niet meer te verstrekken*.

Voor meer uitleg over of om u op een van deze rechten te beroepen, gelieve u intern te richten tot privacy@sintjozefhumaniora.be. Bij eventuele disputen of twijfel, kan u zich ook wenden tot de toezichthoudende autoriteit inzake privacy en de verwerking van persoonsgegevens:https://www.gegevensbeschermingsautoriteit.be/

3.2 Gerechtvaardigd belang

Een aantal verwerkingen hebben een 'gerechtvaardigd belang' als grondslag:
- toezicht op telecommunicatie;
- de in § 2.4 vermelde doorgifte van jouw gegevens aan onderwijsinspectie.

3.3 Geautomatiseerde besluitvorming

Op Sint-Jozef Humaniora worden noch leerlingen, noch ouders onderworpen aan eender welke vorm van geautomatiseerde besluitvorming.

3.4 Al dan niet verstrekken van gegevens

De in § 2.2 en § 2.3 vermelde gegevens moeten, indien van toepassing, verstrekt worden om de inschrijving op Sint-Jozef Humaniora te kunnen starten. Met uitzondering van die gegevens waar expliciet toestemming voor nodig is.

Bijlage 2: Privacyverklaring voor personeelsleden

Privacyverklaring (personeel) – Sint-Jozef Humaniora

Wegens de wetgeving inzake informatieveiligheid en privacy, willen wij u informeren over de verwerkingen die wij met uw persoonsgegevens uitvoeren, en de beleidsmaatregelen die wij nemen om deze te beschermen.

1 Verantwoordelijken

Het schoolbestuur, S.O. Karel-de-Goede vzw, is de verwerkingsverantwoordelijke voor alle personeelsgegevens. Op Sint-Jozef Humaniora is er een aanspreekpunt informatieveiligheid aangeduid, dat gemakkelijk te contacteren is via privacy@sintjozefhumaniora.be. Het aanspreekpunt informatieveiligheid en/of de directie van Sint-Jozef Humaniora kan voor advies en ondersteuning terecht bij de 'data protection officer' (DPO) van de onderwijskoepel.

2 Verwerkingen

2.1 Verwerkingsdoeleinden

Op Sint-Jozef Humaniora verwerken wij personeelsgegevens omwille van de volgende doelen:

- personeelsrekrutering;
- personeelsadministratie;
- personeelsbeheer (o.m. evaluatie);
- loonadministratie;
- public relations;
- toezicht op telecommunicatie;
- camerabewaking.

2.2 Verwerkte personeelsgegevens

Om u te werk te stellen, te begeleiden en op te volgen in Sint-Jozef Humaniora is het noodzakelijk dat wij de volgende gegevens verwerken:

- identificatiegegevens (*met i.h.b. een pasfoto, het rijksregisternummer, gezinssamenstelling*);
- persoonlijke kenmerken (*met i.h.b. geboortedatum, geboorteplaats, geslacht, nationaliteit*);
- privé contactgegevens (*met i.h.b. telefoonnummer(s), adresgegevens, email*);
- loongegevens (*met i.h.b. werkstation, opdracht(en), barema, salaris*);
- loopbaangegevens (*met i.h.b. uittreksel strafregister, getuigschriften, diploma's en bekwaamheidsbewijzen, voorgaande werkgevers (in het onderwijs), dienstanciënniteit, TADD, statutaire benoeming, verlofstelsels*);
- loopbaanbegeleiding (*met i.h.b. lesobservaties, functionerings- en evaluatiegesprekken, gevolgde bijscholingen, verslagen pedagogische begeleiding*);
- aanwezigheid en discipline (*met i.h.b. afwezigheidsbewijzen, berispingen, blamen, tucht*);
- afbeeldingen (*die niet administratief gebruikt worden*);
- bewakingsbeelden.

2.2 Ontvangers

- Het departement onderwijs is, via het werkstation bij AgoDi, een ontvanger van een deel van uw personeelsgegevens;

- De scholengemeenschap S.O. Karel-de-Goede vzw ontvangt uw loopbaan- en loongegevens omwille van hun bevoegdheden inzake TADD, statutaire benoemingen, mutaties en reaffectaties.
- bij verificatie krijgt de onderwijsverificateur mogelijk toegang tot bepaalde loopbaan- en loongegevens;
- bij inspectie is het mogelijk dat een onderwijsinspecteur ook toegang vraagt tot bepaalde personeelsgegevens.

2.4 Verwerkers

Op Sint-Jozef Humaniora worden onderstaande platformen gebruikt bij de verwerking van personeelsgegevens:
- Informat
- Smartschool
- Integreat
- MoneySafe
- Google (Apps for Education en Drive)

2.5 Voorwaarden

Uw gegevens zullen verwerkt worden zolang u bij ons te werk gesteld bent. Daarna worden ze verwijderd, geanonimiseerd of gearchiveerd conform de geldende regelgevingen.
Indien we bepaalde gegevens langer zouden willen bewaren, dan zullen we u dat melden en uw expliciete toestemming ervoor vragen.
Meer informatie over de beleidsmatige aanpak inzake privacy en informatieveiligheid op Sint-Jozef Humaniora kan u raadplegen op www.sintjozefhumaniora.be of opvragen via: privacy@sintjozefhumaniora.be

3 Rechten inzake privacy

3.1 Rechten uitoefenen

U kan zich steeds op onderstaande rechten beroepen:
- recht op informatie: *u mag vragen welke gegevens van u er verwerkt worden en wie er toegang toe heeft (zie ook verwijzing in § 2.5), waarom de school die persoonsgegevens nodig heeft of gebruikt en hoe lang ze bewaard worden*;
- recht op inzage: *u mag steeds de gegevens die de school van u heeft, inkijken a.d.h.v. een kopie*;
- recht op verbetering: *als u fouten in uw gegevens vindt, mag u vragen om dit aan te passen. U kan ook aanvullingen toevoegen aan uw gegevens*;
- recht op gegevenswissing: *u kan vragen dat gegevens, die niet (meer) strikt noodzakelijk zijn voor de school, permanent en volledig verwijderd worden*;
- recht op beperking van de verwerking: *als u bezwaar hebt (zie verder) tegen de verwerking van bepaalde gegevens, kan u vragen om deze verwerking te stoppen*;
- recht op overdraagbaarheid van gegevens: *als u bepaalde gegevens wenst over te dragen naar een nieuwe school of andere werkgever, dan faciliteert de school dit (in de mate van het mogelijke)*;
- recht van bezwaar: *als u niet akkoord gaat met de grondslag van een verwerking of met de manier waarop bepaalde gegevens van u verwerkt worden, kan u zich hiertegen verzetten*;
- recht om niet te worden onderworpen aan geautomatiseerde besluitvorming: *wanneer de school algoritmes gebruikt om, zonder tussenkomst van mensen, bepaalde gevolgen te trekken uit (een deel van) uw gegevens (zie § 3.3), dan kan u zich hiertegen verzetten*;

- recht om zijn/haar toestemming in te trekken: *indien men u voor bepaalde verwerkingen de toestemming gevraagd heeft, kan u ten allen tijde kiezen om deze niet meer te verstrekken*.

Voor meer uitleg over of om u op een van deze rechten te beroepen, gelieve u intern te richten tot privacy@sintjozefhumaniora.be. Bij eventuele disputen of twijfel, kan u zich ook wenden tot de toezichthoudende autoriteit inzake privacy en de verwerking van persoonsgegevens: https://www.gegevensbeschermingsautoriteit.be/

3.2 Gerechtvaardigd belang

Een aantal verwerkingen hebben een 'gerechtvaardigd belang' als grondslag, namelijk:
- toezicht op telecommunicatie;
- de in § 2.3 vermelde doorgifte van uw gegevens aan onderwijsinspectie.

3.3 Geautomatiseerde besluitvorming

Op Sint-Jozef Humaniora worden personeelsleden niet onderworpen aan eender welke vorm van geautomatiseerde besluitvorming.

3.4 Al dan niet verstrekken van gegevens

De in § 2.2 vermelde gegevens moeten, indien van toepassing, verstrekt worden om het arbeidscontract op Sint-Jozef Humaniora te kunnen aangaan. Met uitzondering van:
- afbeeldingen (voor public relations).

Deel 3 Wachtwoordbeleid

3.1 Inleiding

Een goed beveiligingsbeleid dient zich aan omdat steeds meer privacygevoelige gegevens gedigitaliseerd worden, vanuit verschillende locaties toegankelijk zijn en online worden gedeeld. Een wachtwoordbeleid en extra beveiliging om toegang te hebben tot uw toestel voorkomt identiteitsdiefstal, *phishing* en *hacking*. Als uitgangspunt stellen we dat elke gebruiker toegang heeft tot alle informatie die ze nodig hebben om hun taak naar behoren uit te oefenen, maar hen ook alle toegang ontzegt tot informatie die een gebruiker niet nodig heeft.

Deze nota valt onder de eindverantwoordelijkheid van S.O. Karel de Goede vzw.

3.2 Toegangsbeheer

De directeur van de school is verantwoordelijk voor het gebruikersbeheer van de organisatie. Gebruikersbeheer houdt het aanmaken van gebruikers, toekennen van rechten en stopzetten van rechten in.

De school houdt een toegangsmatrixprocedure bij die een inventaris bevat van alle rollen en rechten gekoppeld aan personeelsleden en leerlingen in de school. Aan de hand van dit overzicht kan men een beveiligingsbeleid verder uitwerken rond volgende pijlers:

3.2.1 Authenticatie

Authenticatie is het proces waarbij je je identiteit gaat bewijzen (ben je wel diegene die je beweert te zijn). De school sensibiliseert en maakt afspraken om het inlogproces en –procedures en dus de toegang tot gevoelige data optimaal te beveiligen.

- Betrokkenen wordt informatie aangereikt hoe ze wachtwoorden veilig aanmaken en correct gebruiken.
- De school bepaalt waar een dubbele authentificatiemethode van toepassing is.

3.2.2 Autorisatie

Autorisatie is een proces waarbij onderzocht wordt of je voldoende rechten hebt of toestemming hebt voor hetgeen je wilt doen.

3.2.3 Auditing (controleerbaarheid)

Auditing (*controleerbaarheid*) is het proces waarmee je kan nagaan wie wat waar, wanneer en waarmee doet.

3.3 Wachtwoorden

Wachtwoorden zorgen er mee voor dat de toegang tot applicaties goed beveiligd is. Het is dus van belang om een sterk beleid op te zetten om het inlogproces en -procedures te beheren. Op Sint-Jozef Humaniora werken we er continu aan om leerkrachten en leerlingen het belang van sterke wachtwoorden bij te brengen.
Een wachtwoordbeleid heeft als doel enkele bepalingen op te leggen rond het correct gebruik van wachtwoorden om de toegang tot gevoelige data (waaronder privacy gevoelige persoonsgegevens) te beveiligen middels een wachtwoord.

3.3.1 Wachtwoordbepalingen

- Hoe langer een wachtwoord hoe beter. Het wachtwoord moet minstens 8 karakters hebben. Beter nog is om te werken met een wachtwoordzin (bijvoorbeeld: IkGaSinds2015NaarDeSchool)
- Mix hoofdletters, kleine letters en tekens door elkaar: gebruik volgende tekens in het wachtwoord:
  - Hoofdletters
  - Kleine letters
  - Cijfers
  - Niet-alfanumerieke karakters
- Verander minstens 1 keer per schooljaar je wachtwoord
- Gebruik verschillende wachtwoorden voor verschillende applicaties
- Geef het wachtwoord niet door, op geen enkele wijze aan niemand.
- Schrijf het wachtwoord niet op: niet op papier, niet elektronisch in jouw GSM of PC.
- Verzend nooit een wachtwoord via email of een ander communicatiesysteem. (Niemand van Sint-Jozef Humaniora zal ooit je wachtwoord, om eender welke reden, op deze manier opvragen.)
- Gebruik andere wachtwoorden dan privé-wachtwoorden.
- Bewaar je wachtwoord niet in de browser.

3.3.2 Wachtwoordbeheer

- Na 10 pogingen om in te loggen in een digitaal schoolplatform wordt het account vergrendeld.
- Laat de computer nooit onbeheerd achter maar vergrendel het scherm of log uit.

3.3.3 Wat doen bij vermoeden van misbruik?

Misbruik kan ontvreemding of onrechtmatig gebruik van een wachtwoord zijn.
- Verander het wachtwoord onmiddellijk
- Neem direct contact op met het aanspreekpunt informatieveiligheid, de dienst ICT en/of de systeembeheerder. Meldpunt datalekken: privacy@sintjozefhumaniora.be

Deze personen gaan na of er sprake is van een misbruik en proberen zo nodig de schade te herstellen.

3.4 Gebruik van two-factor authenticatie

Als je echt met veel privacygevoelige persoonsgegevens werkt, is vaak een combinatie van gebruikersnaam en wachtwoord niet voldoende veilig. Daarom bestaan er two-factor authenticatiemethodes.
Deze systemen zijn veel veiliger en worden binnen Sint-Jozef Humaniora dan ook toegepast voor directie en smartschoolbeheerders die aan de meest privacygevoelige gegevens binnen de onderwijsinstelling kan.

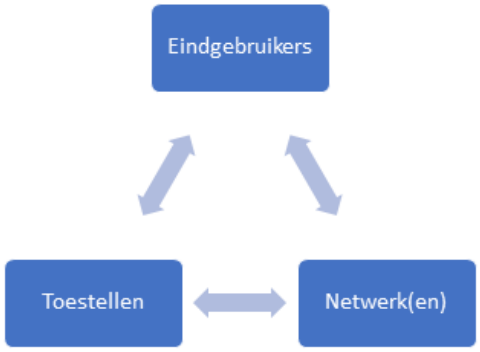
Deel 4 Toestellenbeleid

4.1 Inleiding

4.1.1 Algemeen

In een eenvoudige interpretatie zijn er drie aspecten van een modern ICT-netwerk om rekening mee te houden inzake beschikbaarheid, integriteit en vertrouwelijkheid:

- **(Eind)gebruikers** = *personen*
- **Toestellen** = *desktops, laptops, maar ook tablets, smart-phones, … en ook: servers*
- **Netwerk(en)** = *de verbinding(en) tussen de toestellen onderling en toestellen en gebruikers.*



Deze beleidsnota omschrijft de manier waarop Sint-Jozef Humaniora controle op elk van deze aspecten uitvoert.
Deze nota valt onder de eindverantwoordelijkheid van S.O. Karel de Goede vzw.

4.1.2 Algemene bepalingen

Ongeacht het "type" toestel of netwerk, kan Sint-Jozef Humaniora een aantal maatregelen nemen om:

- te herkennen wanneer het "gewone" verkeer gemonitord, onderschept, nagebootst of gewijzigd wordt.
- het geheel te monitoren of via logboeken handelingen bij te houden voor analyse of eventueel naar bewijslast toe.
- in deze logboeken een aantal **identificatieparameters** te registreren. Er vinden geen ongeoorloofde inzages of systematische analyses plaats op deze gegevens. Enkel bij gegronde vermoedens van inbreuken kunnen hierop gerichte en/of willekeurige controles uitgevoerd worden. Alle informatie hier aangaande wordt strikt vertrouwelijk behandeld.

4.2 Netwerkbeveiliging en -controle

4.2.1 Bekabeld netwerk en servers

Met het "bekabelde netwerk" bedoelen we het geheel van componenten die de netwerkverbindingen maken en beheren, zoals: routers, switchen, hubs, kabels, servers, modems, …
De algemene maatregelen (zie hierboven) worden toegepast.
Wachtwoorden op de netwerkcomponenten worden systematisch gewijzigd t.o.v. de "default" waarden, of te gemakkelijke combinaties. De gekozen wachtwoorden voldoen aan alle afspraken uit het ***wachtwoordbeleid***.

4.2.2 Wifi-netwerk

Voor personeel, leerlingen en gasten is wifi voorzien op Sint-Jozef Humaniora.

De algemene maatregelen (zie hierboven) worden toegepast.

Het netwerkverkeer dat via het draadloze netwerk verloopt, wordt *niet* versleuteld. Het raadplegen, bewerken enz. van persoonsgegevens wordt dan ook ten stelligste afgeraden, tenzij er een andere vorm van versleuteling gehanteerd wordt (*bv. https i.p.v. http*).

4.3 Beveiliging en controle op internetverkeer

Op Sint-Jozef Humaniora is er, zowel voor de toestellen die eigendom zijn van de school als op bepaalde andere toestellen, een internetverbinding mogelijk.
Als organisatie is Sint-Jozef Humaniora verantwoordelijk voor het algehele dataverbruik, en voor alles wat er met / via deze internetverbinding gebeurt. Daarom hanteert de school ook hier een aantal regels en controles.

De algemene maatregelen (zie hierboven) worden toegepast.

De beheerders, noch de elektronische controlesystemen en de logboeken, hebben toegang tot de inhoud van persoonlijke berichten (zoals messaging, email, intern communicatiesysteem, …).

4.4 Beveiliging en controle op toestellen van de school

Onder "toestellen" van de school rekenen we zowel *desktop computers, laptops, tablets* als (eventuele) werk-*smartphones* die eigendom zijn van de school.

4.4.1 Algemeen

De volgende beveiligingsregels resp. -controles kunnen hierop (tegelijkertijd) toegepast worden:

- Het internetverkeer en gebruikte toepassingen wordt, op verscheidene niveaus, gecontroleerd inzake bv. bezochte doelsites, uitgaand verkeer, capaciteit maar ook veiligheid van de toepassing, het al dan niet veranderen van systeeminstellingen (gerelateerd aan beveiliging resp. prestaties, enz.).
- Het zo vlot mogelijk "draaiend" houden van alle hardware en het netwerk is belangrijk. Dit is onmogelijk als gebruikers de systeem- of beveiligingsinstellingen veranderen. Er worden op Sint-Jozef Humaniora dan ook verschillende maatregelen genomen om dit te verhinderen. Het doelbewust veranderen van systeem- of beveiligingsinstellingen is verboden.

Dit beleid wordt gecombineerd met een aantal monitoring tools en/of (lokale) logboeken, d.w.z. manieren om de handelingen bij te houden voor analyse of eventueel naar bewijslast toe.

Op Sint-Jozef Humaniora worden er bepaalde *tools* gebruikt die de actieve vensters en/of het *realtime* beeldscherm van de eigen toestellen kunnen monitoren. De doeleinden hiervan zijn louter en alleen pedagogisch.
Het is in het bijzonder leerkrachten en ondersteunend personeel *niet* toegestaan om zonder concreet vermoeden van doelbewuste en ernstige inbreuken, schermafdrukken te bewaren, een scherm op te nemen of een scherm over te nemen zonder toestemming van de betrokkene.

- Leerkrachten en ondersteunend personeel kunnen, in het kader van hun uit te oefenen taak, de actieve vensters, geopende websites en/of het beeldscherm zien. Het is niet uitgesloten dat de inhoud van **persoonlijke berichten** (ontvangen en/of verzonden) leesbaar is, alhoewel dit nooit het doel op zich zal zijn. Al deze medewerkers behandelen de informatie strikt vertrouwelijk, en bewaren deze niet.

- Het is, met dezelfde tools, wel toegestaan dat de beheerders, directie en eventueel andere personeelsleden die hiervoor bevoegd geacht worden, de schermen bewaren (als een schermafdruk of als een opname). Zij doen dit enkel bij een concreet vermoeden van doelbewuste en ernstige inbreuken en alle informatie wordt strikt vertrouwelijk behandeld. Onbevoegde medewerkers hebben geen toegang tot de schermafdrukken of opnames.

4.4.2 Vergrendeling, encryptie en wissen van op afstand

De mobiele toestellen (d.w.z. *laptops, pda's, tablets, smartphones*) die bepaalde personeelsleden gebruiken maar die eigendom zijn van Sint-Jozef Humaniora, dienen extra beveiligd te worden indien er persoonsgegevens op bewaard, bekeken of verwerkt worden. In het bijzonder wordt er een vergrendeling aan de hand van wachtwoord, *pincode, swipe code*, vingerafdruk of andere authenticatie toegepast.

Voor personeelsleden en derden (CLB) die toegang hebben tot gevoelige persoonsgegevens op het toestel in kwestie geldt bovendien:
- Encryptie van opslagmedia (indien mogelijk);
- Optie om te lokaliseren of te wissen van op afstand, in geval van diefstal of verlies (indien mogelijk).

4.5 Beveiliging en controle op toestellen van eindgebruikers zelf

Op Sint-Jozef Humaniora is het mogelijk om, via het netwerk of wifi van de school (zie ook § 2), gebruik te maken van eigen toestellen. Het is de bedoeling dat deze maximaal gebruikt worden om taken uit te voeren, gerelateerd aan de onderwijsinstelling.

Ook thuis kan men gebruik maken een persoonlijk toestel waarbij er toch enkele aandachtspunten zijn:

4.5.1 Algemeen

Inzake het meebrengen van een eigen toestel op school worden dezelfde maatregelen genomen zoals de toestellen van de school.

4.5.2 Vergrendeling, encryptie, antivirusbeveiliging, *backups* en wissen van op afstand

De mobiele toestellen (d.w.z. laptops, pda's, tablets, smartphones) van medewerkers, waarop persoonsgegevens van Sint-Jozef Humaniora bewaard, bekeken of verwerkt worden, dienen extra beveiligd te worden. Dit beleid vraagt die medewerkers dan ook om de volgende maatregelen op deze toestellen in acht te nemen:
- Er wordt een vergrendeling aan de hand van wachtwoord, pincode, swipe code, vingerafdruk of andere authenticatie gevraagd.
- Er wordt gevraagd om een te allen tijde up-to-date antivirusprogramma te gebruiken.
- Het is belangrijk dat uw toestellen steeds geüpdatet zijn met de laatste patches en updates van het besturingssysteem.

- Backups dienen genomen, bewaard en beheerd te worden zoals in het respectievelijke beleid vastgelegd.

Voor personeelsleden en derden (CLB) die toegang hebben tot gevoelige persoonsgegevens op het toestel in kwestie wordt daarenboven het volgende gevraagd:
- Encryptie van opslagmedia (indien mogelijk);
- Optie om te lokaliseren of te wissen van op afstand, in geval van diefstal of verlies (indien mogelijk)

4.5.3 Verwisselbare media (o.a. usb-stick)

De instelling maakt afspraken om personeelsleden veiliger te laten omgaan met verwisselbare media.
- We adviseren om bij verwisselbare media gegevens te versleutelen als er lesvoorbereidingen, toetsen, proefwerken, leerlingengegevens en/of personeelsgegevens op staan.
- Gevoelige (leerling- of personeels-)gegevens worden niet op verwisselbare media getransporteerd.
- Verwisselbare media met privégegevens worden best niet op school gebruikt.

4.5.4 Aandachtspunten voor het gebruik van uw thuiscomputer voor schoolgerelateerd werk.

Het betreft toestellen in uw bezit zoals:
- de thuiscomputer
  - ➢ *desktop* of *laptop*
  - ➢ *Windows, Mac, Linux,* …
- persoonlijke *laptop* (dus geen eigendom of onder beheer van de school, b.v. *leasing*)
  - ➢ thuisgebruik en/of op school
- persoonlijke *tablet*
- persoonlijke *smartphone*, gsm, …

Richtlijnen: personeelsleden bewaken:
- een afzonderlijke account (tegenover andere gezinsleden, thuisbewoners)
- een voldoende toegangsbeveiliging
- backups en het *up-to-date* houden (besturingssysteem, antivirus en *malware*).

Deel 5 Backupbeleid

5.1 Inleiding

5.1.1 Situering

Voor de gegevens die een bepaald niveau van beschikbaarheid en/of integriteit vereisen, is een goed uitgestippeld backupbeleid noodzakelijk. Deze principes gelden zowel voor gegevens die zich op NAS-en, servers, *clients*, eigen toestellen, andere locaties, in de *cloud*, … bevinden

Deze nota valt onder de eindverantwoordelijkheid van S.O. Karel de Goede vzw.

5.1.2 Enkele begrippen

UPS (*uninterrupted power supply*) Noodstroomvoorziening	*Aangesloten systemen en opslagmedia worden gedurende enkele minuten van stroom voorzien bij pannes of spanningsfluctuaties. Dit zorgt ervoor dat gegevens in het werkgeheugen en/of cache nog kan weggeschreven worden voordat het system afgesloten moet worden.*
Redundantie	*Het algemene principe waarbij een systeem, opslag of netwerkverbinding zo opgebouwd wordt, dat indien nodig een ander systeem overneemt. In principe mogen eindgebruikers hier niets van merken. Het "eerste" systeem dient zo snel mogelijk terug hersteld te worden.*
Backups	*Het nemen van geregelde kopieën, op een andere locatie en medium, zodat bij eventueel verlies of diefstal de gegevens in kwestie hersteld kunnen worden. De aard, frequentie, enz. van de backups wordt bepaald door de classificatie van de gegevens in kwestie. Dit proces kan volledig geautomatiseerd gebeuren.*
Synchronisatie	*Gegevens bevinden zich op verschillende locaties en media, maar een onderlinge netwerkverbinding zorgt ervoor dat beide kopieën hetzelfde zijn. Aanpassingen gebeuren m.a.w. steeds in beide kopieën tegelijk. Het systeem zorgt ervoor dat aanpassingen bijgehouden worden in het geval dat de verbinding (even) weg valt, om deze bij het herstellen van de verbinding zo snel mogelijk samen te voegen.*

5.2 Stroomvoorziening

De Sint-Jozef Humaniora zorgt in de mate van haalbaarheid voor een redundante opstelling van stroomvoorziening.

5.3 Internetverbinding

De Sint-Jozef Humaniora streeft er naar om een continue internetverbinding te voorzien.

5.4 Backups

De Sint-Jozef Humaniora streeft er naar om een perfomant *backup*-plan uit te werken, rekening houdend met de '*best practices'*:

- een dagelijkse *backup* van data
- een *backup* op een andere plaats
- een '*offsite' backup*.

5.5 Brandveiligheid

De Sint-Jozef Humaniora zorgt voor afdoende brandbeveiligingsmaatregelen.

Deel 6 Toegangsmatrices

6.1 Inleiding

6.1.1 Situering

In deze nota bepalen we het gebruikersrechtenbeleid op Sint-Jozef Humaniora. Hiermee bedoelen we welke gebruikers(groepen) welke toegangen hebben tot bepaalde gegevens.

Deze nota valt onder de eindverantwoordelijkheid van S.O. Karel de Goede vzw.

6.1.2 Gebruikersgroepen

Alle dragers, platformen, systemen en het netwerk die binnen Sint-Jozef Humaniora gebruikt worden, vallen onder het IVP-beleid. Dit houdt in dat elk van deze dragers, platformen, systemen en het netwerk voorzien zijn van **beveiligingsgroepen**, waartoe de respectievelijke gebruikers behoren na authenticatie (zie het ***toestelbeleid*** en ***wachtwoordbeleid***).

De volgende gebruikersgroepen worden hierbij gehanteerd:
- *ICT-coördinatoren*
- *CLB-medewerkers*
- *Ondersteuners*
- *Directieleden*
- *Leerlingenbegeleiders*
- *Leerkrachten*
  - *Die les geven aan betrokken leerling*
  - *Die geen les geven aan betrokken leerling*
- *Administratief medewerkers*
  - *Die bevoegd zijn om (in welbepaalde zin) leerlinggegevens te verwerken*
  - *Die bevoegd zijn om (in welbepaalde zin) personeelsgegevens te verwerken*
  - *Die hier niet voor bevoegd zijn*
- *Ouder(s) of voogd, stiefouder(s)*
- *Betrokkene zelf*
- *Derden (bv. onderhoudspersoneel, externe betrokkenen)*

Deze groepen worden globaal gehanteerd binnen het IVP-beleid van Sint-Jozef Humaniora. Mogelijks bestaan er, voor welbepaalde gevallen of toepassingen, nog specifiekere beveiligingsgroepen.

6.1.3 Gebruikersrechten

De algemeen gehanteerde gebruikersrechten zijn:
- Blanco: geen toegang (*men kan de gegevens niet opvragen of zien. Ze worden ook niet in overzichten of dergelijke vermeld*);
- L: leestoegang (*men kan alles zien, maar niets verwijderen, toevoegen of aanpassen*);
- W: wijzig- of schrijftoegang (*men kan alles zien, items toevoegen en aanpassen*);
- VB: volledig beheer (*dit wil zeggen dat men de toegangsrechten, van zichzelf en van anderen, kan aanpassen*).

6.2 Toegangsmatrices

De Sint-Jozef Humaniora heeft een toegangsmatixprocedure waarin alle gebruiksrechten gedefinieerd worden voor elke gebruikersgroep. Deze toegangsmatrixprocedure wordt jaarlijks opnieuw bekeken en geëvalueerd. Volgende onderdelen worden in opgenomen:

- Gegevens van leerlingen
- Gegevens van ouder(s), stiefouder(s) of voogd(en)
- Gegevens van personeelsleden
- Gegevens van oud-leerlingen
- Gegevens van oud-personeelsleden
- Gegevens van derden

Deel 7 Lijst met afkortingen

- AIV Aanspreekpunt Informatieveiligheid
- AVG Algemene Verorderening Gegevensbescherming
- CIV Cel Informatieveiligheid
- DPO Data Protection Officer
- GBA Gegevensbeschermingsautoriteit
- GDPR General Data Protection Regulation
- IVP Informatieveiligheid en privacy