Beleidsverklaring Informatieveiligheid

1. Inleiding

Informatie en digitale middelen zijn belangrijke pijlers in de ondersteuning van het onderwijs. De stijgende digitalisering heeft als gevolg dat onderwijsinstellingen steeds meer gebruik maken van digitale middelen en systemen, zowel voor de administratie en het opvolgen van de leerlingen, het beheer van personeels- en andere gegevens als voor het lesgeven zelf. Deze informatie wordt niet enkel geregistreerd maar ook uitgewisseld/overgedragen met andere diensten (bv. Departement Onderwijs) en tussen systemen onderling. Dit bevordert enerzijds de efficiëntie van de eigen werking en de samenwerking met andere organisaties, maar anderzijds mogen we ook niet blind zijn voor een aantal risico's.

Ons pedagogisch project is een maatschappelijk project waarin **BSGO De Esdoornschool** wil mee bouwen aan de samenleving van de toekomst. Het GO! stelt het **samen leren samenleven** als een kernopdracht voorop, en benadrukt daarmee dat alle mensen in onze samenleving over alle verschillen heen met elkaar verbonden zijn door gemeenschappelijke grondrechten en democratische basiswaarden. Het universele recht op onderwijs veronderstelt dat de samenleving in maximale ontplooiings- en participatiekansen voorziet voor elk individu, volgens zijn of haar mogelijkheden. We zetten in op onze kernwaarden: respect, oprechtheid/eerlijkheid, gelijkwaardigheid, maar ook openheid, engagement en betrokkenheid. Vanuit respect voor onze lerenden, medewerkers en betrokkenen bij ons onderwijs, hebben we ook aandacht voor de bescherming van hun privacy.

De uitdagingen zijn groot. De aard van de dreigingen en risico's op inbreuken wordt steeds complexer en het aantal steeds groter. Dit noopt tot adequate maatregelen voor de omgang met en bescherming van informatie -zowel analoog als digitaal, de middelen om deze informatie te verwerken en de locaties waar met deze informatie wordt omgegaan.

Het stijgend gebruik van internet en sociale media, de groeiende cybercriminaliteit en de toenemende media-aandacht rond incidenten, maakt dat mensen zich bewuster worden van hun privacy en de noodzaak om deze te beschermen. Bovendien verplicht wet- en regelgeving rond gegevensbescherming elke organisatie die persoonsgegevens verwerkt, aandacht te besteden aan een veilige omgang met deze gegevens. Leerlingen, medewerkers, ouders en andere betrokkenen hebben recht op een veilige omgeving waarbinnen hun gegevens zorgvuldig en correct worden verwerkt.

Het belang van informatieveiligheid wordt reeds langer onderkend in onze organisatie. zet dan ook in op de uitbouw, validatie, implementatie en communicatie van een informatieveiligheidsbeleid in al haar instellingen.

2. Wat is informatieveiligheid

Samengevat kan je informatieveiligheid omschrijven als het beschermen van informatie en –systemen tegen

- ongeautoriseerde toegang, gebruik, bekendmaking
- onopzettelijke vernietiging of wijziging
- verlies/diefstal

met het oog op

- het verzekeren van de confidentialiteit, integriteit en beschikbaarheid van informatie
- het vermijden van inbreuken.

We spreken over informatie en –systemen in de ruime zin van het woord. Het spreekt vanzelf dat persoonsgegevens hier een onderdeel van zijn, die conform de wet- en regelgeving beschermd moeten worden. 'Privacy' is integraal onderdeel van informatiebeveiliging.

Informatieveiligheid is in de eerste plaats een organisatorisch vraagstuk. Het raakt de bedrijfsvoering en vraagt daarom om een organisatorische visie, focus en draagvlak. Het technisch luik heeft hierin natuurlijk een sterk karakter

Informatieveiligheid bevindt zich op het snijvlak van:

- het juridische: wet- en regelgeving
- het organisatorische: beleid, structuur, processen, gedrag
- het technische: fysieke beveiliging en ICT

3. Doel en reikwijdte

Doel van het beleid:

- Respect voor de privacy van leerlingen, ouders, medewerkers en andere betrokken bij de werking van **BSGO De Esdoornschool**
- Het onderhouden en verbeteren van de informatieveiligheid binnen **BSGO De Esdoornschool**
- het verzekeren van de continuïteit van de werking en dienstverlening
- het naleven van wet- en regelgeving
- waarborgen van de privacy (correcte omgang met persoonsgegevens)

Het beleid is van toepassing op alle medewerkers, leerlingen/cursisten, ouders, bezoekers, tijdelijk personeel en andere personen betrokken bij de werking van onze instellingen.

Het beleid omvat de processen, onderliggende informatie en -systemen in de meest brede zin van het woord. Het raakt alle onderdelen van de organisatie van **BSGO De Esdoornschool**, zowel de fysieke locaties, de digitale systemen op interne en externe locaties als de analoge en digitale gegevensverzamelingen die gebruikt worden.

4. Uitgangspunten

De belangrijkste beleidsuitgangspunten van het beleid:

- Het beleid vertrekt vanuit respect voor alle personen betrokken bij het onderwijsgebeuren en de werking van **BSGO De Esdoornschool** en sluit zo aan bij het PPGO!.
- Het informatieveiligheidsbeleid dient het garanderen van de betrouwbaarheid, continuïteit, integriteit en authenticiteit van informatie (en –systemen).Het informatieveiligheidsbeleid binnen **BSGO De Esdoornschool** sluit aan bij haar missie, strategische doelen en zal in deze snel veranderende tijden mee evolueren met de organisatie.
- Er wordt voldaan aan alle relevante wet- en regelgeving.
- De rollen en verantwoordelijkheden van alle betrokkenen worden duidelijk gedefinieerd/vastgelegd.
- Informatiebeveiliging is en blijft een verantwoordelijkheid van iedereen maar in het bijzonder van de leidinggevenden en het management.

- Veilig en betrouwbaar omgaan met informatie is een taak van iedereen. Er wordt ingezet op bewustwording zodat verantwoord en bewust gedrag een attitude worden bij alle medewerkers.
- De beleidslijnen worden vertaald naar praktische procedures en richtlijnen.
- Informatieveiligheid vertrekt vanuit risicomanagement zodat risico's tijdig, consistent en effectief kunnen worden aangepakt.
- Er wordt gestreefd naar een goede balans tussen beveiliging enerzijds en functionaliteit/werkbaarheid/gebruiksgemak anderzijds.
- Uitbouwen en implementeren van een informatieveiligheidsbeleid is een continu proces, waarbij periodiek wordt geëvalueerd en bijgestuurd.
- Er is kruisbestuiving met organisatiebeheersing/kwaliteitsmanagement, projectmanagement en bedrijfscontinuïteit.
- Informatieveiligheid wordt ingebed in de werking en processen en vraagt dus een eigen structuur binnen de organisatie.

5. Organisatie

In het uitbouwen en implementeren van een informatieveiligheidsbeleid zijn verschillende rollen en verantwoordelijkheden te onderscheiden.

Eindverantwoordelijke: verantwoordelijk voor het uitwerken, uitdragen, implementeren, evalueren van en controle op het beleid binnen de instelling en het zorgvuldig en rechtmatig verwerken van persoonsgegevens

Informatieveiligheidsconsulent: verantwoordelijk voor het uitwerken van het centraal beleid en uitrollen naar het meso- en lokaal niveau (resp. de scholengroepen en onderwijsinstellingen). Geldt als centraal aanspreekpunt en biedt ondersteuning aan de aanspreekpunten van het meso- en lokaal niveau.

Functionaris voor de gegevensbescherming: ziet toe op de gegevensverwerkingen binnen de organisatie en is contactpersoon inzake verwerking en bescherming van persoonsgegevens.

Informatieveiligheidscel: orgaan waarbinnen de strategie, concrete aanpak, voortgang en knelpunten worden vastgelegd en beheerd.

Aanspreekpunt informatieveiligheid scholengroep: stuurt de implementatie van het informatieveiligheidsbeleid in de scholengroep en onderwijstellingen op lokaal niveau aan, is aanspreekpunt binnen de scholengroep en contactpersoon voor de directie, algemeen directeur en informatieveiligheidsconsulent/DPO

Aanspreekpunt informatieveiligheid in de onderwijsinstelling: neemt, samen met de directie, de implementatie van het informatieveiligheidsbeleid in de onderwijsinstelling op, is aanspreekpunt binnen de onderwijsinstelling en contactpersoon voor het aanspreekpunt informatieveiligheid van de scholengroep en de directie

Medewerker: verantwoordelijk voor het toepassen van de richtlijnen en procedures bij de dagelijkse werkzaamheden en het melden van incidenten.

Ook externe medewerkers/diensten die (tijdelijk) opdrachten voor de **BSGO De Esdoornschool** opnemen, moeten de richtlijnen van het beleid naleven.

6. Aanpak

Het GO! stelt een centraal informatieveiligheidsbeleid vast. De organisatie-brede focus krijgt een borging in een meerjarenplan; de gerealiseerde acties in een jaarverslag. Dit beleid en zijn uitrol worden centraal door de Raad van het GO! goedgekeurd.

Op niveau van **BSGO De Esdoornschool** wordt een specifiek beleid vastgesteld voor de eigen context. De informatieveiligheidscel van **BSGO De Esdoornschool** geeft het beleid vorm en voert alle acties uit die horen bij een degelijk informatieveiligheids- en privacybeleid (o.a. uitvoeren van risico-analyse, gegevensbeschermingseffectbeoordeling, actieplannen, wettelijk verplichte instrumenten, incidentmelding- en registratie, -behandeling, melding, rapportage…).

Centraal in het beleid staat de risico-gebaseerde aanpak. Op basis van de risicoanalyse zal het niveau van de beveiligingsmaatregelen worden bepaald, rekening houdend met de classificatie van de gegevens. De centrale kwaliteitscriteria hierbij zijn beschikbaarheid, integriteit en vertrouwelijkheid.

De directie neemt een actieve rol en eigenaarschap op om dit beleid organisatorisch in te bedden, te implementeren en op te volgen. De aanpak krijgt een borging in een meerjarenplan; de gerealiseerde acties in een jaarlijkse rapportage.

Bij het uitwerken van het beleid wordt **BSGO De Esdoornschool** ook ondersteund door het aanspreekpunt informatieveiligheid van de scholengroep.

Er wordt binnen **BSGO De Esdoornschool** actief ingezet op bewustwording zodat veilig en correct omgaan met informatie, -systemen en digitale middelen een vanzelfsprekende attitude wordt. Kennis hierover wordt o.m. gerealiseerd via bewustwordingsacties, een gedragscode en specifieke richtlijnen.
Bovendien wordt voorzien in een procedure voor het melden van incidenten. Iedereen is hiervan op de hoogte zodat zo snel mogelijk de juiste oplossing voor het incident kan worden voorzien, dergelijke incidenten kunnen worden voorkomen. Ook vanuit incidentregistratie wordt verder aan bewustwording gewerkt.

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het proces. Leidinggevenden en proceseigenaren nemen hierin hun rol op en sturen medewerkers bij indien nodig. Regelmatige rapportage biedt input voor bijsturing en creëren van bewustwording.

Het informatieveiligheids- en privacybeleid wordt opgenomen in het kwaliteitsdenken van de organisatie. Het beleid wordt op regelmatige tijdstippen aan een kritische blik onderworpen en bijgestuurd waar nodig.

Doorheen het proces van uitwerken, implementeren, evalueren en bijsturen zal, waar nodig, met andere instanties en netwerken worden overlegd en samenwerkt.