

PRIVAATHEIDSBELEID VAN (VOEG DIE NAAM VAN DIE SKOOL IN)

Posadres van die skool:

Straatadres van die skool:

Telefoonnommer van die skool:

E-posadres van die skool:

Inligtingsbeampte: _____ (Prinsipaal)

E-posadres:

Adjunkinligtingsbeampte: _____ (Deur die prinsipaal benoem)

E-posadres:

1. Inleiding

- 1.1 (Voeg die naam van die skool in) ("die skool") is 'n openbare skool ingevolge die Suid-Afrikaanse Skolewet (SASW), 1996 (Wet 84 van 1996), en word bestuur en beheer ingevolge die bepalings van die SASW asook die taal en toelatingsbeleid wat daarvolgens opgestel is. Die medium van onderrig by die skool is (voeg taal(tale) van onderrig in). Die skool bied onderrig vanaf graad (voeg graad in) tot (voeg graad in).
- 1.2 Die skool moet sekere inligting oor individue en regspersone (gesamentlik verwys na as "datasubjekte") versamel en gebruik. Artikel 1 van die Wet op die Beskerming van Persoonlike Inligting (POPIA), 2013 (Wet 4 van 2013) omskryf 'n "datasubjek" as "*die persoon op wie persoonlike inligting betrekking het*". 'n Datasubjek kan leerders, opvoeders, kliënte/diensverskaffers van die skool, verskaffers, sakekennisse, werknemers, vrywilligers en ander persone waarmee die skool 'n verwantskap het of 'n kontrak mag aangaan, insluit.
- 1.3 Hierdie beleid beskryf hoe hierdie inligting versamel, verwerk, en bewaar moet word om aan die skool se persoonlike inligtingsbeskermingstandaarde en aan die wet te voldoen.
- 1.4 Die skool beskou die wettige en toepaslike verwerking van alle persoonlike inligting as van deurslaggewende belang vir suksesvolle dienslewering en noodsaaklik vir die behoud van vertroue tussen die skool, datasubjekte en entiteite/agentskappe/sakeondernemings/persone wat met die skool skakel. Die skool bekragtig en voldoen dus ten volle aan die beginsels van die POPIA en die regulasies wat ingevolge die wet uitgevaardig is.
- 1.5 Die prinsipaal, (voeg die naam van die prinsipaal in), is die inligtingsbeampte van die skool, en hy/sy kan skriftelik gekontak word oor enige kwessies wat met die POPIA verband hou.
- 1.6 Die adjunkinligtingsbeampte, (voeg die naam van die adjunkinligtingsbeampte in), van die skool is deur die prinsipaal gedelegeer en hy/sy kan skriftelik gekontak word.
- 1.7 Definisies word aan die einde van hierdie beleid uiteengesit om die betekenis van die terme wat gebruik word, te verduidelik.

2. Doel

- 2.1. Die privaatheidsbeleid verseker dat die skool:
 - a) aan die POPIA, 2013 (Wet 4 van 2013) voldoen;
 - b) die regte van datasubjekte, soos omskryf, beskerm;
 - c) eerlik is oor hoe dit persoonlike inligting van datasubjekte versamel, behou, bewaar, vernietig, geskrap, en verwerk word; en
 - d) die skool en datasubjekte se regte teen die risiko van 'n sekuriteitsverbreking bewaar.

3. Beleidsverklaring

- 3.1. Ingevolge die verpligtinge wat deur die POPIA opgelê is, moet die skool die privaatheid van datasubjekte beskerm. Die POPIA beskryf hoe die skool die persoonlike inligting van datasubjekte moet versamel, verwerk en bewaar.
- 3.2. Hierdie beginsels is van toepassing, ongeag of die inligting elektronies, op papier of op ander materiaal bewaar word.
- 3.3. Om aan die POPIA te voldoen, is die volgende belangrike privaatheidsbeginsels van toepassing. Die persoonlike inligting moet:
 - a) redelik en wettig verwerk word;
 - b) vir die spesifieke, voorgeneemde doel verkry word;
 - c) genoegsaam, bruikbaar en nie onrealisties wees nie;
 - d) korrek wees en gereeld bygewerk word;
 - e) nie vir langer as nodig gehou word nie;
 - f) verwerk word ooreenkomstig die regte van datasubjekte;
 - g) op gepaste wyses bewaar word; en
 - h) nie buite Suid-Afrika oorgedra word nie tensy die land of gebied ook seker maak dat daar 'n voldoende vlak van beskerming is.

4. Omvang

- 4.1. Hierdie beleid is van toepassing op alle werknemers by die skool, beide permanente en tydelik, asook werknemers wat op kontrakbasis werk, afrigters, vrywilligers, en ander persone wat gemagtig is om toegang te verkry tot persoonlike inligting wat deur die skool gehou word.
- 4.2. Die bepalinge van die beleid is van toepassing op beide die ter plaatse en afstandsverwerking van persoonlike inligting en inligting deur 'n assistent of gedelegeerde persoon.

4.3. Dit beheer alle sakebedrywighede wat die verwerking van persoonlike inligting asook spesiale persoonlike inligting, vir of namens die skool behels. Hierdie persoonlike inligting en spesiale persoonlike inligting mag, onder andere, die volgende insluit:

4.3.1. Persoonlike inligting:

- a) Inligting wat verband hou met die ras, gender, geslag, swangerskap, huwelikstatus, nasionaliteit, etniese/sosiale oorsprong, kleur, seksuele oriëntasie, ouderdom, liggaamlike gesondheid/geestesgesondheid, welstand, gestremdheid, geloof, integriteit, mening, kultuur, taal en geboorte van die persoon.
- b) Inligting wat verband hou met die onderrig van die mediese, finansiële, kriminele of indiensnemingsgeskiedenis van die persoon.
- c) Enige identifiserende nommer, simbool, e-posadres, woonadres, telefoonnommer, inligting oor ligging, aanlyn identifiseerder of ander spesifieke aanduiding wat die persoon identifiseer.
- d) Biometriese inligting van die persoon.
- e) Die persoonlike menings, sieninge of voorkeure van die persoon.
- f) Korrespondensie wat deur die persoon gestuur is wat implisiet of uitdruklik privaat of vertroulik is of verdere korrespondensie wat die inhoud van die oorspronklike korrespondensie sal blootstel.
- g) Die standpunt van 'n ander individu oor die persoon.
- h) Die naam van die persoon, indien dit met ander persoonlike inligting van die persoon verband hou, verskyn, of as die openbaarmaking van die naam self inligting oor die persoon openbaar sal maak.

4.3.2. Spesiale persoonlike inligting:

- a) Die godsdienstige/filosofiese oortuigings, ras/etniese oorsprong, vakbondlidmaatskap, politieke oortuiging, gesondheid/sekslewe of biometriese inligting.
- b) Die kriminele gedrag van 'n persoon wat verband hou met die beweerde pleging van enige misdryf en enige verrigtinge ten opsigte van enige misdryf wat na bewering deur 'n persoon gepleeg is, of die afhandeling van sodanige verrigtinge.

5. Risiko's

5.1. Hierdie beleid help om die skool en datasubjekte teen veiligheidsrisiko's te beskerm, ingeslote:

- a) **Verbreking van vertroulikheid** – inligting wat onvanpas gedeel word;
- b) **Versuim om keuses aan te bied** – alle datasubjekte moet die vryheid hê om te kies hoe die skool inligting oor hulle gebruik, waar die persoonlike inligting

nie versamel word of gedeel word ingevolge 'n wet of 'n ooreenkoms tussen die datasubjek en die skool nie;

- c) **Skade aan reputasie** – die skool of die datasubjek kan skade aan hulle reputasie opdoen indien kuberkrakers suksesvol toegang tot die persoonlike inligting van datasubjekte verkry; en
- d) **Verlies aan persoonlike inligting.**

6. Verantwoordelikhede

6.1. Almal wat vir of saam met die skool werk is verantwoordelik om te verseker dat die persoonlike inligting van datasubjekte toepaslik versamel, bewaar en verwerk word om die vertroulikheid, integriteit en beskikbaarheid daarvan te verseker.

6.2. Almal binne die skool moet toesien dat alle personeel wat persoonlike inligting bestuur of toegang daartoe het aan hierdie beleid voldoen. As deel van die jaarlikse beplanningsproses van die skool, moet die beheerliggaam en lede van die skoolbestuurspan prosedures op hulle gebiede hersien om nakoming van hierdie beleid en POPIA te verseker.

6.3. Almal wat met persoonlike inligting werk, moet seker maak dat dit ooreenkomstig hierdie beleid en die privaatheidsbeginsels hanteer en verwerk word.

6.4. Die volgende persone het verantwoordelikhede op die volgende hoofgebiede:

6.4.1. Die inligtingsbeampte is volkome verantwoordelik daarvoor om toe te sien dat die skool sy wettlike verpligtinge nakom.

6.4.2. Die inligtingsbeampte/adjunkinligtingsbeampte is verantwoordelik daarvoor om:

- a) op die hoogte te bly van inligtingsbates en persoonlike inligtingsbeskermingsverantwoordelikhede, risiko's en verwante kwessies;
- b) alle persoonlike inligtingsbeskerming van beleide en prosedures te hersien;
- c) persoonlike inligtingsbeskermingsopleiding en raad aan die toepaslike werknemers en persone wat deur hierdie beleid gedek word, te reël; en
- d) enige kontrakte of ooreenkomste met derde partye wat persoonlike inligting namens die skool mag versamel, hanteer, bewaar of vernietig, na te gaan en goed te keur.

6.4.3. Die inligtingsbeampte/adjunkinligtingsbeampte is verantwoordelik vir die hantering van versoeke van datasubjekte (ook "datasubjekversoeke tot toegang" genoem) wat die persoonlike inligting wat die skool oor hulle het wil sien. Die identiteit van enigeen wat 'n datasubjekversoek tot toegang rig, moet geverifieer word voordat enige persoonlike inligting bekendgemaak word.

6.4.4. [Voeg die naam van die bewaarder van die inligting in] is verantwoordelik daarvoor om:

- a) te verseker dat alle inligtings- en kommunikasietegnologie- (IKT-) bates wat vir verwerking van persoonlike inligting gebruik word aan geskikte veiligheidstandaarde voldoen;
- b) gereelde kontrole en skanderings uit te voer om te verseker dat sekuriteitshardeware en sagteware behoorlik funksioneer; en
- c) enige dienste deur derde partye wat die skool oorweeg om te gebruik om persoonlike inligting te verwerk, byvoorbeeld, wolkrekenardienste, te evalueer.

7. Algemene riglyne

- a) Die enigste persone wat toegang kan kry tot enige persoonlike inligting wat deur hierdie beleid gedek word behoort diegene te wees wat **dit vir werk of wettige doeleindes nodig het**.
- b) Persoonlike inligting **moet nie informeel gedeel word nie** en moet nooit deur die gebruik van rekeninge op sosiale media soos Facebook, LinkedIn, Google Plus, WhatsApp, ensovoorts, gedeel word nie.
- c) Wanneer toegang tot persoonlike inligting nodig is, kan werknemers dit van die inligtingsbeampte of sy/haar gedelegeerde persoon versoek.
- d) Die skool **sal opleiding** aan alle werknemers **bied** om hulle te help om hul verantwoordelikhede vir die hantering van persoonlike inligting te verstaan.
- e) Deur voorsorgmaatreëls te tref en die riglyne wat hier uiteengesit is, te volg, moet werknemers alle persoonlike inligting **veilig** bewaar.
- f) Veilige **wagwoorde moet gebruik word**, en dit moet nooit gedeel word nie.
- g) Persoonlike inligting **moet nie** aan ongemagtigde persone, óf binne die skool óf daarbuite, **bekendgemaak word nie**.
- h) Persoonlike inligting moet **gereeld hersien en bygewerk word** as dit verouderd mag voorkom. As dit nie meer vir die voorgenome doel daarvan verlang word nie, moet dit geskrap en ooreenkomstig die beskikkingsproses beskik word.
- i) Werknemers **moet** die inligtingsbeampte of sy/haar gedelegeerde **om hulp vra** as hulle onseker is oor enige aspek van die beskerming van persoonlike inligting.

7.1. Versameling van inligting

7.1.1. Die skool versamel inligting om sy diensleweringmandaat te ondersteun.

7.1.2. Waar moontlik, word persoonlike inligting direk van datasubjekte versamel, en altyd in ooreenstemming met die POPIA.

- 7.1.3. Die skool versamel die volgende soorte inligting:
- a) Inligting oor leerders en hulle ouers wat deur leerders, hul ouers en ander persone verskaf is.
 - b) Inligting oor werksaansoeke, werknemers, vrywilligers en besoekers wat deur werksaansoekers, werknemers, vrywilligers, besoekers en ander verskaf is.
- 7.1.4. Die skool versamel inligting op verskeie wyses, ingeslote:
- a) van aangesig tot aangesig en telefonies;
 - b) uit elektroniese en drukstukdokumente, werksaansoeke, e-posse, fakture, toelatingsvorme, briewe aan die skool, toestemmingsvorme (byvoorbeeld, toelatings, uitstappies of leerderondersteuningsdienste), die skool se webwerf of skoolbeheerde sosiale media ingeslote;
 - c) deur aanlynhulpmiddels, soos aansoeke en ander sagteware wat deur die skool gebruik word; en
 - d) deur enige geslote kringtelevisiekameras wat op die skoolpersele aangetref word (indien van toepassing).
- 7.1.5. Die skool se hoofdoel vir die versameling van persoonlike inligting oor leerders en hulle ouers is om:
- a) leerders te onderrig; en
 - b) leerders se sosiale en emosionele welstand te ondersteun.
 - c) aan regsvereistes te voldoen, ingeslote om:
 - i. redelike stappe te doen om die risiko van redelike voorsiene skade aan leerders, werknemers en besoekers te verminder (sorgsame plig);
 - ii. redelike wysigings aan te bring vir leerders met gestremdhede, waar van toepassing; en
 - iii. 'n veilige en beskermde leeromgewing te verskaf.
 - d) die skool in staat te stel om:
 - i. met ouers in gesprek te tree kwessies oor leerders by die skool en die pogings en prestasies van leerders te vier; en
 - ii. die goeie orde en bestuur van die skool te handhaaf.
 - e) die Wes-Kaap Onderwysdepartement (WKOD), die Departement van Basiese Onderwys (DBO), die ouditeur-generaal (OG) of enige ander gemagtigde persone in staat te stel om:
 - i. die doeltreffende bestuur, hulpbronverwerwing en administrasie van die skool te verseker;
 - ii. wetlike funksies en pligte na te kom;
 - iii. die WKOD se beleide, dienste en funksies te beplan, te befonds, te monitor, te reguleer en te evalueer;
 - iv. aan verslagdoeningsvereistes te voldoen; en
 - v. voorvalle by skole te ondersoek en/of op enige wettige eise te reageer.

- f) Die skool se hoofdoel van die versameling van inligting oor werknemers, vrywilligers en werksaansoekers is om:
 - i. aansoekers se geskiktheid vir indiensneming of vrywillige werk te assesseer;
 - ii. indiensneming of vrywillige plasing te administreer;
 - iii. aan verskeie wetlike verpligtinge te voldoen, indiensneming en kontraktuele verpligtinge, beroepsgesondheidswette en veiligheidswette ingeslote, en om voorvalle te ondersoek; en
 - iv. op wetlike eise teen die skool of die WKOD te reageer.

7.2. **Klassifisering van inligting**

- 7.2.1. [Voeg die naam van die eienaar van die inligting in] klassifiseer inligting ooreenkomstig sy regsvereistes, waardes, deurslaggewendheid en sensitiwiteit vir ongemagtigde openbaarmaking, modifikasie of verlies.
 - a) Persoonlike inligting word gewoonlik as KONFIDENSIEEL geklassifiseer.
 - b) Spesiale persoonlike inligting en kinders se inligting word gewoonlik as PRIVAAT geklassifiseer.

7.3. **Gebruik van inligting**

- 7.3.1. Wanneer toegang tot persoonlike inligting verkry en gebruik word, kan dit 'n baie groot risiko van verlies, korrupsie of diefstal inhou. Dus is die volgende belangrik:
 - a) Werknemers moet seker maak dat wanneer hulle met persoonlike inligting werk, **hulle rekenaarskerms gesluit is** wanneer hulle dit sonder toesig laat.
 - b) Persoonlike inligting moet nie **informeel gedeel word nie**.
 - c) Alle persoonlike inligting wat via **e-pos** gestuur is (as 'n aanhangsel of in die teks van 'n e-pos) moet as sensitief beskou word en as sodanig bewaar word. Dit moet nie aan iemand buite die skool gestuur word nie tensy dit deur die inligtingsbeampte goedgekeur is. Dit sluit die aanstuur van sodanige e-posse aan 'n werknemer se eie persoonlike e-posrekening in.
 - d) Voordat 'n e-pos aan 'n medewerknemer gestuur word, bevestig by die inligtingsbeampte dat die ontvanger toegelaat is om toegang daartoe te hê aangesien nie alle gebruikers binne die skool toegang tot dieselfde inligting het nie.
 - e) Data moet **geënkripteer word voordat dit elektronies oorgedra word**.
 - f) Persoonlike inligting moet **nooit buite Suid-Afrika oorgedra word nie** sonder dat daar bevestig is dat die land waarna dit oorgedra word 'n voldoende vlak van beskerming van persoonlike inligting kan verseker nie.
 - g) Werknemers **moenie afskrifte van persoonlike inligting van datasubjekte op hulle eie rekenaars bewaar nie**. Verkry altyd toegang tot die sentrale afskrif van enige persoonlike inligting en werk dit by.

7.4. **Bewaring van inligting**

7.4.1. Hierdie beginsels beskryf hoe en waar persoonlike inligting veilig bewaar moet word. Vrae oor die veilige bewaring van persoonlike inligting kan aan die inligtingsbeampte/adjunkinligtingsbeampte gerig word.

7.4.2. Wanneer persoonlike inligting op **papier bewaar word**, moet dit op 'n veilige plek gehou word waar ongemagtigde persone dit nie kan sien of toegang daartoe kan kry nie. Hierdie riglyne is ook van toepassing op persoonlike inligting wat gewoonlik elektronies bewaar word, maar wat om een of ander rede gedruk is.

- a) Indien dit nie benodig word nie, moet die papier of lêers in 'n **geslote laai of liasseerkas gehou word**. As die inligting as **PRIVAAT** geklassifiseer is, moet toegang tot die inligting **geënkripteer** wees en aangeteken word.
- b) Werknemers moet seker maak dat papier en drukstukke **nie gelos word waar ongemagtigde persone dit kan sien nie**, soos by 'n drukker of fotostaatmasjien.
- c) **Drukstukke wat persoonlike inligting bevat, moet onmiddellik versnipper word** en veilig van ontslae geraak word as dit nie meer vir die voorgenome doel verlang word nie.

7.4.3. Wanneer persoonlike inligting **elektronies bewaar word**, moet dit teen ongemagtigde toegang, onbeplande skrapping en kwaadwillige pogings deur kuberkrakers beskerm word:

- a) Alle elektroniese bewaring verg toegangskontroles soortgelyk aan dié wat verwerk is en lêerbeskermingsmeganismes soos **enkodering** moet gebruik word.
- b) Alle elektroniese toegang moet **aangeteken word**.
- c) Persoonlike inligting moet slegs op **aangewese aandrywers en bedieners** bewaar word en slegs na **goedgekeurde wolkrekenadienste** oorgedra word.
- d) Die bewaring van persoonlike inligting op enige ander fisiese toestel, ingeslote, maar nie beperk nie tot, Universal Serial Bus- (USB-) geheuestokkie (geheuestafie), eksterne hardeskywe, kompakskywe (CD's) of digitale videoskywe (DVD's) moet **vooraf** deur die inligtingsbeampte of sy/haar gedelegeerde **goedgekeur** word.
- e) Indien persoonlike inligting **op verwyderbare media gestoor word** (soos 'n geheuestokkie, eksterne hardeskyf, CD of DVD) moet die lêers geënkripteer word, deur 'n wagwoord beskerm word, en die media moet veilig toegesluit word wanneer dit nie gebruik word nie.
- f) USB-geheuestokkies (geheuestafies) wat gevind word of as 'n bemarkingsitem uitgedeel is, moet nie in enige rekenaar ingeprop word nie, aangesien hierdie toestelle versteekte, skadelike programmatuur of virusse mag bevat.

- g) Alle verlore of gesteelde toestelle (verwyderbare media ingeslote) moet onmiddellik by die inligtingsbeampte aangemeld word.
- h) Waar redelik uitvoerbaar, moet bedieners wat persoonlike inligting bevat, op **'n veilige plek geplaas word**, weg van die algemene kantoorruimte.
- i) Daar moet **gereeld reserwekopieë** van elektroniese lêers wat persoonlike inligting bevat, **gemaak word**. Hierdie reserwekopieë moet gereeld getoets word ooreenkomstig die skool se standaard prosedures vir die maak van reserwekopieë.
- j) Alle bedieners, rekenaars en ander elektroniese toestelle wat persoonlike inligting bevat, moet deur **goedgekeurde sekuriteitsagteware en 'n brandmuur** beskerm word.

7.5. Akkuraatheid van data

- 7.5.1. Die POPIA verg dat die skool redelike stappe doen om te verseker dat persoonlike inligting akkuraat en bygewerk bly.
- 7.5.2. Alle werknemers wat met persoonlike inligting werk is daarvoor verantwoordelik om redelike stappe te doen om te verseker dat dit so ver moontlik akkuraat en bygewerk bly.
 - a) Elektroniese lêers wat persoonlike inligting bevat moet op **so min moontlike plekke** bewaar word. Werknemers moet nie enige onnodige bykomende datastelle skep nie.
 - b) Werknemers moet **van elke geleentheid gebruik maak om te verseker dat persoonlike inligting bygewerk word**, byvoorbeeld, deur 'n persoon se besonderhede te bevestig wanneer hulle bel.
 - c) Die skool sal dit **vir datasubjekte maklik maak om hulle persoonlike inligting**, waaroor die skool in beheer is of besit, **by te werk**.
 - d) Persoonlike inligting moet **bygewerk word wanneer onakkuraathede ontdek word**.

7.6. Wegdoening

- 7.6.1. 'n Veilige beskikkingshouer of snippermasjien moet gebruik word om werksdokumente en afskrifte volgens 'n algemene beskikkingsinstruksie te vernietig.
- 7.6.2. Afskrifte van persoonlike inligting, asook spesiale persoonlike inligting, wat as **PRIVAAT** geklassifiseer en **elektronies bewaar is**, moet óf permanent vernietig óf oorgeskryf word.
- 7.6.3. Die beskikking van alle oorspronklike en elektroniese lêers moet uitgevoer word ooreenkomstig die skool se rekordbestuursbeleid.

8. Datasubjektoegangsversoeke

- 8.1. Alle datasubjekte wie se persoonlike inligting deur die skool gehou word, is geregtig om:
- a) te vra **watter inligting** die skool oor hulle hou, waarom en met wie hulle dit deel;
 - b) te vra **hoe om toegang** daartoe **te verkry**;
 - c) ingelig te word oor **hoe om dit bygewerk te hou**; en
 - d) ingelig te word oor hoe die skool **sy verpligtinge nakom ingevolge die POPIA**.
- 8.2. Indien 'n datasubjek in aanraking kom met die skool en hierdie inligting aanvra, word dit **'n datasubjektoegangsversoek** genoem.
- 8.3. Datasubjektoegangsversoeke moet na die inligtingsbeampte/adjunk--inligtingsbeampte verwys word.
- 8.4. Die skool verskaf slegs skoolverslae en gewone skoolkommunikasie aan ouers wat 'n wettige reg op daardie inligting het.
- 8.5. 'n Gedelegeerde verteenwoordiger is in sekere omstandighede nie geregtig op toegang tot inligting oor die leerder nie. Hierdie omstandighede sluit in wanneer toegang nie in die leerder se belang is nie, die skool se plig om die leerder te versorg, geskend kan word, dit teen die wense van 'n leerder mag wees of op onredelike wyse 'n impak op die privaatheid van 'n ander persoon mag hê.

9. Openbaarmaking (deel) van persoonlike inligting

9.1. Interne openbaarmaking

- 9.1.1. Persoonlike inligting word in die algemeen binne die skool gedeel waar dit wetlik toegelaat word vir redelike en toepaslike onderrigdoeleindes. Maar selfs binne die skool is toegang beperk tot dié werknemers of derde partye wat toegang benodig om hulle toegekende funksies uit te voer.
- 9.1.2. Die skool openbaar inligting, wat soos volg met POPIA ooreenstem:
- a) vir 'n primêre doel soos uiteengesit in paragraaf 7.1;
 - b) vir 'n verwante sekondêre doel na redelike verwagting, byvoorbeeld, om die beheerliggaam in staat te stel om sy doelstellings, funksies en magte uit te voer;
 - c) met toestemming, ingeslote toestemming wat op toelatings- en ander vorms gegee is (die inligting versamel sal nie bekendgemaak word buite die WKOD sonder toestemming nie, tensy sodanige openbaarmaking wettig of redelik in die omstandighede is);
 - d) waar nodig, om die ernstige bedreiging van die volgende te verminder of verhoed:

- i. 'n persoon se lewe, gesondheid, veiligheid of welstand of;
- ii. die publiek se gesondheid, veiligheid of welstand;
- e) wanneer deur die wet vereis of geregverdig, byvoorbeeld, om aan 'n hofbevel, dagvaarding of lasbrief gehoor te gee;
- f) om 'n onwettige aktiwiteit te ondersoek of aan te meld, of waar redelik nodig vir 'n spesifieke doel van wetstoepassing, ingeslote die voorkoming van of ondersoek na 'n strafbare oortreding of ernstige misdryf;
- g) vir die DBO, die WKOD, die OG en enige ander gemagtige persone se navorsing of skoolstatistieke; en/of
- h) om 'n wettige eis in te stel of daarop te reageer.

9.2. Eksterne openbaarmaking

9.2.1. Openbaarmaking buite die skool vind slegs ingevolge 'n ooreenkoms plaas, soos toegelaat, of deur die wet of 'n regsproses, of met die toestemming van die datasubjek of 'n bevoegde persoon indien die datasubjek 'n minderjarige is.

9.2.2. Die POPIA laat toe dat persoonlike inligting sonder die toestemming van die datasubjek of 'n bevoegde persoon gedeel word as dit op nasionale sekuriteit of strafbare oortredings betrekking het. In hierdie omstandighede sal die inligting wat versoek word, bekendgemaak word. Die inligtingsbeampte/adjunkinligtingsbeampte sal egter seker maak dat die versoek wettig en in ooreenstemming met die POPIA is, en hulp van die inligtingsreguleerder vra, waar nodig.

9.3. Leerderoorplasings tussen gewone openbare skole

9.3.1. Wanneer 'n leerder by 'n ander skool aanvaar word en na 'n ander openbare skool oorgeplaas is, dra die skool inligting oor die leerder na daardie skool toe oor. Dit mag afskrifte oor die leerder se skoolrekords insluit, buiten die leerder se dissiplinêre rekords, ingeslote enige persoonlike inligting oor die leerder se gesondheid, indien nodig, om spesiale ondersteuning aan 'n leerder te verskaf of om spesiale reëlins oor 'n leerder se gesondheid te tref.

9.3.2. Dit laat die skool wat die inligting ontvang toe om voort te gaan met die ondersteuning van die leerder se sosiale en emosionele welstand en gesondheid, en om regsvereistes na te kom.

10. Kennisgewing aan datasubjekte

10.1. Die skool poog om te verseker dat datasubjekte bewus is dat hulle persoonlike inligting verwerk word, en dat hulle begryp hoe die persoonlike inligting gebruik word, wat hul regte ingevolge die POPIA is, en hoe om hierdie regte uit te oefen.

10.2. Vir hierdie doel het die skool 'n privaatheidskennisgewing waarin uiteengesit word hoe persoonlike inligting oor 'n datasubjek versamel en deur die skool gebruik word.

10.3. Die privaatheidskennisgewing is op versoek beskikbaar.

11. Persoonlike inligting van kinders

11.1. Die skool mag nie kinders se persoonlike inligting verwerk nie tensy:

- a) die skool die toestemming van 'n bevoegde persoon het;
- b) dit nodig is vir verpligtinge onder die POPIA en ander wetgewing;
- c) dit 'n vereiste is vir die handhawing van plaaslike en internasionale publiekreg; en/of
- d) dit vir navorsingsdoeleindes nodig is.

12. Waarskuwing aan ouers of bevoegde persone

12.1. Alhoewel wette oor wat die skool en derde partye oor leerders bekend mag maak van toepassing is, is dit nie van toepassing op wat leerders of hulle ouers in die openbaar bekend mag maak nie, wat beteken dat die ouer en die leerder ook 'n verantwoordelikheid het om die leerder se privaatheid te beskerm. Dit wat 'n ouer en/of sy/haar kind op sosiale media plaas, byvoorbeeld, kan deur ander mense gebruik word, ingeslote privaat maatskappye en regsafdwinging in sekere gevalle, en word nie deur die POPIA beskerm nie.

12.2. Ouers en kinders moet die privaatheidsinstrumente op enige webwerf of toepassing wat hulle vir skool/by die huis gebruik, begryp en gebruik om te beperk wie hulle inligting kan besigtig of toegang daartoe verkry (dit sluit in om sterk, veilige en unieke wagwoorde te hê en seker te maak dat daar nooit enigiets aanlyn geplaas word wat hulle nie wil hê met ander gedeel moet word nie, ingeslote regsafdwinging, die skool, tersiêre instellings en huidige of toekomstige werknemers nie).

13. Verpligtend

13.1. Nienakoming van hierdie beleid deur die skool se werknemers kan tot gevolg hê dat daar disiplinêre stappe teen hulle gedoen word. Die gevolge daarvan mag disiplinêre stappe wees wat tot moontlike beëindiging van indiensneming kan lei, en/of regsgedinge om enige verliese van of skade aan die skool te herwin, ingeslote die herwinning van enige boetes of administratiewe strafopleggings wat deur die inligtingsreguleerder ingevolge die POPIA op die skool gelê is.

13.2. Nienakoming van die beleid deur enige ander derde party wat persoonlike inligting namens die skool verwerk, sal in ooreenstemming met die ooreenkoms wat tussen die skool en sodanige derde party bereik is, hanteer word. Die gevolge daarvan

mag die herwinning van enige boetes of administratiewe strafopleggings wat deur die inligtingsreguleerder ingevolge die POPIA op die skool gelê is, insluit.

14. Oorsig

Hierdie beleid moet hersien word wanneer dit nodig word of in die geval van veranderde omstandighede, soos uitsprake deur wetgewing en/of regulasies en begrotingsbeperkings.

Definisies:

adjunkinligtingsbeampte	beteken 'n persoon wat deur die prinsipaal van die skool in sy/haar hoedanigheid as die inligtingsbeampte aangestel is.
bevoegde persoon	beteken 'n persoon wat regsbevoeg is om toe te stem tot enige handeling of besluit wat geneem word ten opsigte van enige aangeleentheid met betrekking tot 'n kind.
datasubjek	beteken die identifiseerbare natuurlike of regspersoon op wie persoonlike inligting betrekking het.
inligtingsbates	beteken die bates wat die skool gebruik om inligting te skep, bewaar, oor te dra, te skrap en/of vernietig om sy onderrigaktiwiteite asook die inligtingstelsels waarmee daardie inligting verwerk word, te ondersteun. Dit sluit die vtogende in: a) Alle elektroniese en nie-elektroniese inligting wat geskep of gebruik is ter ondersteuning van onderrigaktiwiteite ongeag vorm of medium, byvoorbeeld, dokumente op papier, elektroniese lêers, stemkommunikasie, teksboodskappe, fotografiese of videogrepe. b) Alle toepassings, toestelle en ander stelsels waarmee die skool sy inligting verwerk, byvoorbeeld telefone, faksmasjiene, drukkers, rekenaars, netwerke, stempos, e-posse, kitsboodskappe, slimfone en ander mobiele eenhede ("IKT-bates").
inligtingsbeampte	beteken die prinsipaal van die skool.
inligtingsbewaarder	beteken die persoon wat vir die definiëring en inwerkinstelling van sekuriteitsmaatreëls en beheer van alle IKT-bates verantwoordelik is.

inligtingseienaar	beteken 'n persoon wat verantwoordelik is vir, of afhanklik is van die sakeproses wat met 'n inligtingsbater geassosieer word.
persoonlike inligting	<p>beteken inligting aangaande 'n identifiseerbare, lewendige, natuurlike persoon, en waar van toepassing, 'n identifiseerbare, bestaande regspersoon, met inbegrip van, maar nie beperk nie tot</p> <ul style="list-style-type: none"> a) inligting met betrekking tot die ras, gender, huwelikstaat, nasionaliteit, ouderdom, fisiese/geestelike gesondheid, gestremdheid, geloof, kultuur, taal en geboorte van die persoon; b) inligting met betrekking tot die opvoeding, mediese, finansiële, kriminele of werksgegesiedenis van die persoon; c) enige identifiserende nommer, simbool, e-posadres, fisiese adres, telefoonnommer, inligting oor ligging, aanlyn identifiseerder of ander besondere toewysing aan die persoon; d) die biometriese inligting van die persoon; e) die persoonlike menings, sieninge of voorkeure van die persoon; f) korrespondensie gestuur deur die persoon wat vanselfsprekend of uitdruklik van 'n private of vertroulike aard is of verdere korrespondensie wat die inhoud van die oorspronklike korrespondensie aan die lig sal bring; g) die sieninge/menings van 'n ander individu oor die persoon; en h) die naam van die persoon as dit verskyn met ander persoonlike inligting met betrekking tot die persoon of waar die openbaarmaking van die naam op sigself inligting oor die persoon aan die lig sal bring.
verwerking	<p>beteken enige bedrywigheid of aktiwiteit of enige stel bedrywigheide aangaande persoonlike inligting, met inbegrip van:</p> <ul style="list-style-type: none"> a) die insameling, ontvangs, optekening, organisering, insortering, bewaring, bywerking, verandering, herwinning, aanpassing, konsultasie of gebruik;

	<p>b) verspreiding by wyse van oorsending, verspreiding of beskikbaarstelling in enige ander vorm; of</p> <p>c) samesmelting, koppeling, asook inperkings, degradasie, uitwissing of vernietiging van inligting.</p>
<p>spesiale inligting persoonlike</p>	<p>beteken persoonlike inligting oor:</p> <p>a) die geloofs- of filosofiese oortuigings, ras/etniese herkoms, vakbondlidmaatskap, politieke oortuiginge, gesondheid/sekslewe of biometriese inligting; en</p> <p>b) die kriminele gedrag van 'n persoon vir sover dit van toepassing is op die beweerde pleging van enige misdryf of enige verrigtinge ten opsigte van enige misdryf wat na bewering deur 'n persoon gepleeg is of die beskikking van sodanige verrigtinge.</p>
<p>werknemer</p>	<p>beteken enigeen, buiten 'n onafhanklike kontrakteur, wat vir 'n ander persoon werk of wat help met die verrigting van 'n werknemer se sake.</p>