Bijlage E: Programma van eisen ICT-dienstverlening

1	Algemene eisen
1.1	Opdrachtnemer draagt zorg voor één centraal contactpersoon voor Opdrachtgever met vaste back-up.
1.2	Indien medewerkers van de Opdrachtnemer werkzaamheden uitvoeren op locaties van de Stichting waarbij zij in contact komen met kinderen, dienen zij in het bezit te zijn van een geldige Verklaring Omtrent Gedrag (VOG). De VOG mag niet ouder zijn dan twee (2) maanden en dient te zijn afgegeven op basis van screeningsprofiel 84 (Belast zijn met de zorg voor minderjarigen) en/of 86 (Kinderopvang), of de daarvoor in de plaats komende profielen. De Opdrachtnemer overlegt de VOG van de betrokken medewerker(s) op eerste verzoek van de Opdrachtgever, uiterlijk vóór aanvang van werkzaamheden op locatie. De kosten voor het verkrijgen van de VOG zijn voor rekening van de Opdrachtnemer. Daarnaast dient de Opdrachtnemer een doorlopend screeningsproces te hanteren, waarmee wordt gewaarborgd dat alle medewerkers blijvend voldoen aan de integriteits- en veiligheidseisen van de Opdrachtgever. Indien een medewerker niet (meer) over een geldige verklaring beschikt, wordt deze de toegang tot de locaties van de Opdrachtgever ontzegd.
1.3	De Opdrachtnemer zal, op zowel gevraagd als ongevraagd verzoek, advies verstrekken met betrekking tot alle aspecten binnen de scope. Dit met als doel de Opdrachtgever inzicht te verschaffen in innovaties en mogelijke verbeteringen, waardoor de gestelde doelstellingen op een efficiëntere wijze kunnen worden behaald.
1.4	De gegevens in zowel de huidige als de gewenste omgeving blijven eigendom van de Opdrachtgever. De toegepaste instellingen dienen transparant te zijn en eenvoudig overdraagbaar naar een andere beheerder.
1.5	Opdrachtnemer voorziet in een gebruikersinterface die in de Nederlandse taal is.
1.6	Gedurende het gehele eerste jaar van deze Overeenkomst zullen géén prijswijzigingen worden doorgevoerd. Na het eerste jaar van de Overeenkomst zal vanaf 1 juni 2027 een prijswijziging kunnen worden doorgevoerd voor dat komende jaar. Een prijswijziging zal nimmer met terugwerkende kracht gebeuren.
1.7	Prijswijzigingen dienen uiterlijk twee maanden voor het verstrijken van het kalenderjaar te worden aangedragen door Opdrachtnemer ter acceptatie op basis van maximaal het CBS-prijsindexcijfer CAO lonen per uur inclusief bijzondere beloningen, categorie zakelijke dienstverlening, waarbij het prijsniveau staat voor 2024 en gelijk is aan 100. Opdrachtnemer stelt de prijswijziging vast op basis van het prijsindexcijfer en meldt dit schriftelijk bij Opdrachtgever.
2	**Infrastructuur/netwerk**
2.1	Opdrachtnemer is belast met de volledige uitvoering en verantwoordelijkheid van de ICT-dienstverlening, waarbij alle activiteiten die onder systeembeheer en configuratiebeheer vallen, inbegrepen zijn.
2.2	Opdrachtnemer draagt de verantwoordelijkheid voor het beheren van de volledige huidige en toekomstige installed base van Opdrachtgever, zoals beschreven in eis 3.1 tot en met 3.8. Hieronder vallen onder andere, maar niet beperkt tot: multifunctionals (inclusief onderhoud van adresboeken), werkstations (desktops en laptops), devices, switches, touchscreens, routers, software (besturingssystemen, kantoor- en onderwijsapplicaties) en beveiligingssoftware (anti-virus).

2.3	Opdrachtnemer neemt het beheer van alle bestaande systemen over.
2.4	Opdrachtnemer installeert geen servers (data- print of mailservers) op de locaties van Opdrachtgever.
2.5	Opdrachtnemer garandeert dat de aangeboden oplossing kan samenwerken met de huidige en toekomstige software.
3	**Beheer**
3.1	Asset management: Opdrachtnemer is verantwoordelijk voor het complete proces van aanschaf tot afschrijving van IT-middelen van Opdrachtgever. Opdrachtnemer voert activiteiten uit die leiden tot een adequaat administratief beheersproces van IT-middelen. Opdrachtnemer registreert alle aanwezige devices (inclusief kenmerken) van de Opdrachtgever en maakt dit inzichtelijk voor Opdrachtgever. Opdrachtgever kan te allen tijde periodiek (nader af te stemmen) een rapportage opvragen zonder bijkomende kosten.
3.2	Configuratie management: Het beheren van programmastuursystemen (software) en apparatuur door middel van een speciaal informatiesysteem als gereedschap (tool) om wijzigingen (change) te controleren en beheersen en de integriteit van het systeem te waarborgen.
3.3	Change management: Opdrachtnemer maakt gebruik van gestandaardiseerde methoden en procedures om wijzigingen (changes) te kunnen afhandelen, waarbij het onderwijsproces zo min mogelijk wordt onderbroken.
3.4	Incident management: Opdrachtnemer hanteert incident management als proces, waarbij het doel is om een incident terug te brengen naar het normale en overeengekomen kwaliteitsniveau.
3.5	Problem management: Opdrachtnemer is verantwoordelijk voor het volledige proces van het afhandelen van problemen, met als doel storingen en incidenten proactief te verminderen. Hierbij neemt opdrachtnemer ook de verantwoordelijkheid voor het proactief monitoren van de gehele IT-omgeving.
3.6	Release management: Opdrachtnemer is verantwoordelijk voor het plannen en toezicht houden op de uitrol van nieuwe releases voor hard- en software. De planning wordt te allen tijde voorgelegd aan de opdrachtgever.
3.7	Capaciteit management: Opdrachtnemer is verantwoordelijk voor het waarborgen van de juiste capaciteit voor alle IT-middelen om te kunnen voldoen aan de huidige en toekomstige behoeften van opdrachtgever.
3.8	Actieve monitoring, inrichting, beheer en onderhoud, security, incl. apparatuur en vervangingscyclus van Wifi-omgeving en firewalls zijn onderdeel van de opdracht. De huidige AP (Access Points) zijn eigendom van Opdrachtgever en worden onderdeel van de beheer opdracht.
4	**Toegang en beveiliging**
4.1	Opdrachtnemer beheert alle accounts van medewerkers en leerlingen.
4.2	Opdrachtgever doet verzoeken tot het aanmaken van nieuwe gebruikersaccounts. Opdrachtnemer maakt nieuwe accounts aan en koppelt de gewenste rollen en rechten in de Microsoft-omgeving met de landingspagina.
4.3	Opdrachtnemer beschikt over een automatische koppeling met de landingspagina van Opdrachtgever om automatisch (leerling) accounts aan te maken en te blokkeren.
4.4	De Opdrachtnemer draagt bij dat de Opdrachtgever uiterlijk 1 januari 2030 voldoet aan het Normenkader (IBP) voor informatiebeveiliging en privacy, of op het moment dat dit wettelijk verplicht wordt. Opdrachtnemer zal, gevraagd en ongevraagd, adviseren op alle onderdelen binnen het Normenkader (IBP).
4.5	Opdrachtnemer is verantwoordelijk voor het leveren, installeren, configureren, beheren en up-to-date houden van beveiligingssoftware, waaronder, maar niet beperkt

	tot: anti-virus. Het doel van de Aanbestedende Dienst is ervoor te zorgen dat zij beschikt over een veilige IT-omgeving. Opdrachtnemer biedt hier een passende oplossing voor, conform de geldende wet-en regelgeving op elk moment gedurende de contractperiode.
4.6	Opdrachtnemer is verantwoordelijk voor het correct en consequent volgen van de Algemene Verordening Gegevensbescherming (AVG) en toekomstige wettelijke opvolgers. Hierbij wordt voldaan aan alle wettelijke IT-beveiligings- en regelgeving.
4.7	Opdrachtnemer beschikt over een ISO 27001 informatiebeveiligingscertificering.
4.8	Opdrachtnemer is verantwoordelijk voor het firewall beheer.
4.9	Opdrachtnemer mag bemiddelen in de levering van licenties (hardware en software). In dat geval draagt opdrachtnemer zorg voor een correcte tenaamstelling van de software, waarbij de software altijd wordt tenaamgesteld op naam van opdrachtgever.
4.10	Opdrachtnemer realiseert en beheert een storingsvrije toegang naar alle software gedurende alle lesdagen van de Opdrachtgever.
4.11	Opdrachtnemer is verantwoordelijk voor het installeren, configureren, beheren en up-to-date houden van alle software en besturingssoftware.
4.12	De Opdrachtnemer dient expertise te hebben op het gebied van beveiliging en security van ICT-systemen, met aantoonbare ervaring in het werken met onderwijsinstellingen.
4.13	De aangeboden ICT-omgeving dient maximale bescherming te bieden tegen bekende en opkomende bedreigingen, zoals malware, ransomware, phishing en DDoS-aanvallen. Hierbij is het essentieel dat de opdrachtnemer expertise kan aantonen in het implementeren van effectieve beveiligingsmaatregelen.
4.14	Er dient een geïntegreerd authenticatie- en autorisatiesysteem te zijn om de toegang tot systemen en gegevens te beheren. Dit systeem moet sterke wachtwoordbeleidsregels omvatten en de minimaal mogelijkheid bieden voor MFA (Multi-Factor-Authenticatie)
4.15	Er moet continue, 24/7 monitoring zijn van de beveiligingssystemen en het netwerk, met inbegrip van logboekregistratie en analyse. In geval van verstoring wordt de Opdrachtgever direct geïnformeerd.
5	**Servicedesk beschikbaarheid en bereikbaarheid**
5.1	De Opdrachtnemer vervult de SPOC-rol en moet snel, efficiënt en proactief reageren op alle vragen, incidenten en verzoeken van Opdrachtgever met betrekking tot de ICT. Indien nodig wordt er met derden geschakeld. De Opdrachtnemer fungeert als probleemhouder en neemt verantwoordelijkheid voor het oplossen van de gemelde problemen, waarbij heldere communicatie en een minimale impact op het onderwijsproces centraal staan.
5.2	Opdrachtnemer voorziet in een webbased platform waarop Opdrachtgever incidenten, problemen en wijzigingen kan melden. Op elk moment heeft de Opdrachtgever zicht op de status, doorlooptijd en genomen acties met betrekking tot het oplossen van gemelde incidenten, problemen of wijzigingen. Afmelding van deze gemelde zaken gebeurt te allen tijde door de opdrachtgever/melder.
5.3	Opdrachtnemer hanteert gestandaardiseerde procedures, zoals ASL en ITIL, voor de afhandeling van incidenten, problemen en wijzigingen.
5.4	De servicedesk ondersteuning is beschikbaar in de Nederlandse taal.
5.5	De servicedesk van de Opdrachtnemer is beschikbaar voor Opdrachtgever op werkdagen (maandag t/m vrijdag) van minimaal 07:30 uur tot 17:00 uur.
5.6	Opdrachtnemer dient voorafgaand aan elk kalenderjaar een planning van preventieve onderhoudswerkzaamheden te overleggen en te leveren aan Opdrachtgever.
5.7	Opdrachtnemer plant in overleg met Opdrachtgever correctieve onderhoudswerkzaamheden zo spoedig mogelijk in.

5.8	Indien een storing/melding niet onder de verantwoording valt van Opdrachtnemer dan dient dit vooraf gecommuniceerd te worden met Opdrachtgever.
5.9	Opdrachtnemer overlegt een volledige SLA en DAP nadat de voorlopige gunning is ontvangen. In de SLA worden verschillende onderwerpen beschreven, waaronder maar niet beperkt tot: responstijden, escalatieafhandeling, overlegstructuur, beveiligingsbeheer, callintake, changemanagement, configuratiemanagement, releasemanagement, capaciteits- en performancemanagement. Deze SLA en DAP maken integraal deel uit van de Overeenkomst en bevatten de minimale eisen zoals vermeld in de Overeenkomst en de nader overeen te komen KPI's (Key Performance Indicators) om kwaliteit te borgen.
5.10	Opdrachtnemer biedt, indien de storing niet op afstand (remote) opgelost kan worden, on site support aan.
6	**Migratie**
6.1	Opdrachtnemer is verantwoordelijk voor de gehele migratiefase inclusief een voorbereidende training voor alle medewerkers waarbij ze leren hoe de omgeving werkt.
6.2	Opdrachtnemer stelt altijd in overleg met Opdrachtgever een migratie/overgangsdatum vast. Opdrachtgever geeft hier een schriftelijk akkoord voor.
6.3	De migratie wordt uitgevoerd en gepland in nauw overleg met de Opdrachtgever.
6.4	Bij iedere (deel) migratie geeft Opdrachtgever een Go/No Go. In het geval van een No Go beslissing worden de extra kosten niet vergoed door opdrachtgever. Indien een no go beslissing door een derde partij wordt veroorzaakt is Opdrachtnemer niet verantwoordelijk.
6.5	Nazorg is onderdeel van de migratie en wordt niet apart doorbelast aan Opdrachtgever. In de nazorg fase wordt er ook een evaluatiegesprek met Opdrachtgever gehouden. Een basis training is onderdeel van de nazorg fase en dient binnen de migratiekosten zijn inbegrepen.
7	**Rapportage en communicatie**
7.1	Opdrachtnemer en Opdrachtgever evalueren half jaarlijks de IT-dienstverlening. Opdrachtnemer is verantwoordelijk voor het organiseren van dit half jaarlijkse overleg.
7.2	Opdrachtnemer rapporteert periodiek (minimaal 1 keer per kwartaal) over de resultaten van de servicedesk, conform de SLA. Op verzoek van Opdrachtgever overlegt opdrachtnemer te allen tijde.
7.3	Op verzoek van Opdrachtgever overlegt Opdrachtnemer te allen tijde informatie/rapportages zoals in eis 7.2 is omschreven.
8	**Exit plan**
8.1	Op verzoek van Opdrachtgever zullen Partijen binnen 3 maanden of, indien dit op kortere termijn is, voor het einde van de Overeenkomst, gezamenlijk een Exit Plan opstellen. Opdrachtnemer zal alle medewerking verlenen die nodig is bij het invullen van dit Exit Plan. Het exit plan is minimaal 1 maand voor de einddatum gereed.
8.2	Het Exit Plan bewerkstelligt de volledige migratie en/of overstap van de Diensten naar een nieuwe door Opdrachtgever gekozen dienstverlener. Alle werkzaamheden in verband met de migratie en/of overstap zullen geschieden tegen de standaardtarieven van Opdrachtnemer. Partijen zullen ieder de eigen kosten dragen voor het opstellen en bijhouden van het Exit Plan.
8.3	Het Exit Plan bevat in elk geval een volledige omschrijving van: (i) de taken die Opdrachtnemer op zich zal nemen in verband met de overdracht van de Diensten en overige informatie; (ii) de samenwerking tussen Opdrachtnemer enerzijds en Opdrachtgever of een door Opdrachtgever aangestelde derde anderzijds; (iii) het elektronische formaat waarin de relevante informatie ter beschikking zal worden gesteld (waaronder configuraties, Documentatie en codes).

8.4	Tot aan de einddatum voor de Diensten, zoals bepaald in de Overeenkomst, door welke vorm van beëindiging dan ook, blijft Opdrachtnemer volledig verantwoordelijk voor een volledige, tijdige en juiste uitvoering van de Diensten.
9	**Digitale Werk-en Leeromgeving / Landingspagina**
9.1	De Opdrachtnemer biedt een DLWO of vergelijkbare oplossing met geïntegreerde onderwijs platformen aan. Deze maakt onderdeel uit van de inschrijving en zit binnen de prijs per medewerker/leerling inbegrepen.
9.2	De DLWO of vergelijkbare oplossing, moet intuïtief en gebruiksvriendelijk zijn voor zowel docenten als leerlingen.
9.3	De DLWO of vergelijkbare oplossing moet toegankelijk zijn op verschillende apparaten i.c.m. een Office365 account.
9.4	De Digitale Leerweg omgeving of vergelijkbare oplossing op school biedt een veilige omgeving voor alle leerlingen.
9.5	Een volledige Digitale Werk- en Leeromgeving of vergelijkbare oplossing wordt geleverd inclusief koppelingen met relevante onderwijsapplicaties, Single Sign-On, beveiligingsmaatregelen en centraal beheer.
9.6	De Digitale Leerweg omgeving of vergelijkbare oplossing bevat een aanpasbare contentfilter
9.7	Door middel van bijvoorbeeld adresboekscheiding kunnen de contacten van leerlingen worden beperkt
9.8	Het leerkrachtportaal biedt een centrale plek waar alle benodigde informatie beschikbaar is, waaronder onderwijs gerelateerde gegevens, apparaat beheer (via Intune), en toegang tot de helpdesk.
9.9	De DLWO of vergelijkbare oplossing moet ontworpen zijn met een onderwijsgerichte benadering, waarbij bijvoorbeeld de instelling van wachtwoorden mogelijk is op verschillende strengheidsniveaus.
9.10	De DLWO of vergelijkbare oplossing moet de leerkracht de regie geven over de leerlingomgeving en het beheer van apparaten, waaronder de mogelijkheid om Chromebooks zelf in CITO FACET te plaatsen.
9.11	Het moet mogelijk zijn om via het leerkrachtportaal mee te kijken op de leerling device, over te nemen of de activiteiten van de leerling te beheren, bijvoorbeeld door de Toetsmodus in te schakelen.
9.12	De leerkracht moet in staat zijn om zowel zijn eigen portaal als dat van de leerling handig in te delen in categorieën, zodat het overzichtelijker is om specifieke items te vinden.
9.13	Het beheer van alle apparaten (Windows, Apple, Chromebooks) moet eenvoudig zijn voor de scholen.
9.14	Jonge leerlingen moeten op een eenvoudige manier kunnen inloggen, bijvoorbeeld met een plaatjeslogin of optioneel met een QR-code, terwijl oudere leerlingen gebruik kunnen maken van een gebruikersnaam en wachtwoord.