Vraag en antwoord Wegingstafel 10 februari 2026		
Beschikbaar stellen middelen voor ICT-voorzieningen gemeenteraad 2026-2030		
Datum vraag	**Fractie(s)**	**Vraag en antwoord**
	ONS Belang	1. Waarom zijn (niet alle) raadsleden bij dit voorstel betrokken aangezien het hen direct aangaat? Antwoord: Zoals gebruikelijk worden voorstellen m.b.t. de raad geagendeerd in het presidium. De fractievoorzitters kunnen dit bespreken in hun fractie. 2. Gezien het feit dat een iPad makkelijker is in gebruik, krijgen raadsleden die niet handig zijn met een computer hiervoor training? Antwoord: Door het team Informatievoorziening wordt, in afstemming met griffie, een uitvoeringsplan opgesteld voor de ondersteuning van raads- en commissieleden bij het inrichten en in gebruik nemen van de nieuwe ICT-voorzieningen. Dit is dan inclusief uitleg over de afspraken over service en onderhoud binnen de reguliere openingstijden van de ICT Servicedesk. 3. Waarom mogen raads(commissie)leden niet kiezen tussen een iPad of laptop? Antwoord: Om de raadsleden niet te beperken in het uitvoeren van hun werk is gekozen voor een laptop. Denk hierbij aan het opslaan van stukken. 4. In de stukken staat dat de laptops bedoelt zijn voor raadscommissieleden die actief deelnemen aan het raadsplein. Wordt er ook rekening gehouden met het feit dat ongeveer 1 op de 3 beëdigde raadscommissieleden niet tot zelden komt opdagen? Met andere woorden: wanneer komt een raadscommissielid in aanmerking? Antwoord: Om die reden is opgenomen "die actief deelnemen aan". Zoals dat nu het geval is beoordeelt de fractievoorzitter of een commissielid voor een laptop in aanmerking komt. Het uitgangspunt is een veilige werkomgeving. En dus voor een Windows laptop in combinatie met een gemeentelijk e-

		mailadres als gebruikersnaam. Een beveiligingsincident kan door ieder lid veroorzaakt worden. 5. Deze verkiezingen doen er mogelijk 11 partijen mee aan de verkiezingen. Potentieel dus 33 raadscommissieleden. In het voorstel gaat het om 25 raadscommissieleden. Hoe gaat dat verschil gedekt worden? Antwoord: Na de verkiezingen weten we het totaal aantal raadscommissieleden. Het aantal partijen kan ook op slechts 5 of 6 uitkomen. Of niet alle partijen besluiten om 3 raadscommissieleden in te zetten. In dit voorstel is uitgegaan van de huidige situatie. Deze raming kan daarna nog aangepast worden. 6. De waarde van de laptop is een veelvoud van de vergoeding voor een raadscommissielid. Daarnaast wisselt de samenstelling van raadscommissieleden vaak gedurende de komende 4 jaar. Waarom worden ook raadscommissieleden voorzien van een laptop? Antwoord: De kosten en reputatieschade van de gemeente bij een beveiligingsincident kunnen ook een veelvoud zijn van de waarde van een laptop. Ieder raadscommissielid kan een beveiligingsincident veroorzaken. Daarom stellen wij voor dat ieder raads- en commissielid wordt voorzien van veilige apparatuur en software. Bij vertrek van een raadscommissielid dient de apparatuur weer ingeleverd te worden en gaat deze na opschoning en onderhoud naar een opvolger. 7. In de stukken wordt aangegeven dat de laptops en licenties bedoelt zijn vanwege beveiligingsvoorzieningen/eisen. Maar raads(commissie)leden kunnen nog steeds iBabs openen op een (privé)apparaat naar keuze. Het uitdelen van laptops garandeert dus helemaal niet dat vertrouwelijke documenten alleen op goed beveiligde apparaten geopend/bewaard worden. Wat is dan de meerwaarde? Antwoord: De gemeente biedt een veilige digitale werkomgeving aan zodat vertrouwelijke gegevens vertrouwelijk kunnen blijven. Wij kunnen deze apparatuur bij verlies of diefstal op afstand onklaar maken. Door gebruik te maken van speciale overheidslicenties en functionaliteiten van Microsoft beschermen we ons ook juridisch en technisch tegen de meeste risico's. Daarnaast biedt de omgeving ook nog extra functionaliteiten als MS OneDrive en MS Teams voor de raads- en commissieleden.

		Er zijn inderdaad omwegen te bedenken om alsnog op een onveilige manier te werken. Het blijft altijd een risicoafweging tussen gebruikersgemak en veiligheid. Zo is het ook altijd nog mogelijk om mondeling vertrouwelijke informatie te lekken. We gaan er vanuit, net als in de digitale situatie, dat raads- en commissieleden dit niet doen en op een verantwoorde manier omgaan met de informatie van onze gemeenschap. 8. De meeste raadsleden gebruiken een privé email adres. Zij kunnen niet gedwongen worden een emailadres van de gemeente te gebruiken. Wederom de vraag: wat is dan nog de meerwaarde op het gebied van veiligheid? Antwoord: Het feit dat gemeenteraadsleden best veel privé informatie openbaar publiceren (van e-mailadressen tot 06 nummers) is een veiligheidsrisico dat u zelf (mogelijk onbewust) neemt als publiek persoon. Na een bedreiging richting een gemeenteraadslid enige jaren geleden en een jarenlange phishing campagne waarbij gebruik werd gemaakt van openbare gegevens van raads- en bestuursleden zijn wij met het huidige voorstel gekomen. Wij zijn hierin niet alleen er zijn meerdere gemeenten met een soortgelijke aanpak waarbij gemeentelijke apparatuur en software beschikbaar gesteld wordt. Wij kunnen met onze werkomgeving, inrichting en bijbehorende AI-bescherming veel meer maatregelen nemen om dit soort kwaadaardige actoren tegen te gaan. Denk dan aan filtering op kwaadaardige bijlagen, het blokkeren van kwaadaardige verzenders, scannen op malware, etc. Wij vragen u als raad om in te stemmen met dit voorstel. Hierbij gaan wij er ook vanuit dat u gebruik gaat maken van het gemeentelijk e-mailadres voor officiële raads- en commissiezaken. Niet alleen voor uw eigen veiligheid, maar ook voor die van uw collega's en de informatie van de gemeenschap. Accounts voor iBabs worden vanaf de aankomende raadsperiode aangemaakt met behulp van een gemeentelijk e-mailadres en communicatie vanuit de Griffie zal ook naar dat adres plaatsvinden. Of u dit mailadres en de bijkomende functionaliteiten als opslag in MS OneDrive, MS Teams, etc. ook wilt gebruiken voor interne partijcommunicatie dat is geheel aan u.

20-01-2026	LEV	Gebruiksgemak en beveiliging. 1. als je iBabs straks alleen kan gebruiken op je chromebook omdat het alleen compatibel is met Windows werkt het niet meer op je iPad of iPhone. Daarmee ben je best wel beperkt en is naar de mening van LEV geen voordeel te behalen. Beveiliging is goed, misschien dat er iets strakker gekeken moet worden naar wachtwoord en 2FA, vergendelingsinstellingen en maandelijks een securitycheck in te voeren. Maar er zijn echt tal van stappen waar we naar kunnen kijken, deze oplossingen kosten vrijwel niets. Zijn de alternatieven goed onderzocht? Antwoord en/of reactie: Uiteraard is er goed over nagedacht. We gaan niets toepassen dat we ook niet voor de gemeentelijke medewerkers al toepassen. We stappen juist af van Chromebooks omdat deze, ook in de ambtelijke organisatie, niet als gebruikersvriendelijk worden ervaren. We stellen voor over te stappen naar een Windows laptop in combinatie met een M365 account. Een Windows omgeving heeft t.o.v. een Chromebook of iPad als voordeel dat we met de beoogde Microsoft licenties extra juridische, technische en functionele functionaliteiten krijgen om veiliger te kunnen werken. Door gebruik te gaan maken van MS OneDrive en MS Teams bieden we ook extra functionaliteit om als partij(en) samen te werken aan documenten. Deze ontwikkeling is in lijn met wat er door het land heen aan de orde is bij andere gemeenten. Een voorbeeld is Rotterdam. Tot op heden maken onze raadsleden eigenlijk op het beveiligingsniveau van een particulier gebruik van ICT-middelen. Deze zijn niet “in beheer” van de IT-organisatie zoals we dat in ICT-vakjargon noemen. Zo verwachten wij dat er nu geen extra beveiligingsmaatregelen worden genomen die in een zakelijke omgeving normaal zijn. De wereld is echter aan het veranderen. Niet alleen in aantal maar ook in complexiteit nemen de cybersecurity aanvallen toe. Met de komst van AI en de geopolitieke veranderingen worden de risico’s alleen nog maar groter. Vanuit organisaties als de IBD, NCSC en AIVD ontvangen we steeds vaker waarschuwingen voor pogingen vanuit het buitenland om gemeenten aan te vallen. Er is steeds meer aandacht voor het beheer en de beveiliging van informatie. Waar men vroeger stapels papier had en later stukken werden rondgemaild, gaan nu veel documenten, openbaar of vertrouwelijk, via de applicatie iBabs. Veel stukken worden gedownload en opgeslagen op eigen of gemeentelijke hardware. Bij verlies of diefstal lopen we daar een extra risico mee. We hebben met de voorgestelde optie de mogelijkheid om bij verlies of diefstal de machine onklaar maken om zo misbruik uit te sluiten.

		Gedragsregels en een cybersecurity convenant. 2. Wat is er op het gebied van digitale veiligheid al (denk aan cybersecurity-afspraken) en wat er nog nodig (bijv. convenant)? Misschien is de ambtelijke organisatie al met iets bezig? Antwoord en/of reactie: Informatiebeveiliging heeft in onze organisatie al tientallen jaren de volle aandacht. De ontwikkelingen gaan steeds sneller, de kans op een incident en de bijbehorende financiële impact wordt ook steeds groter naarmate we meer gebruik maken van ICT. Op hardware gebied volgen we de best practices door de jaren heen. Van een simpele laptop omgeving met een virusscanner en een firewall tot nu een netwerk en Microsoft omgeving die 24/7 in de gaten wordt gehouden met behulp van AI. Ook op het gebied van wet- en regelgeving wordt alles steeds meer complex. De Cyberbeveiligingswet en BIO 2.0 komen er dit jaar aan. We zijn druk bezig met een programmateam om dit in te voeren. U krijgt hier meer over te lezen in de RIB van de CISO.
20-01-2026	GroenLinks	Vraag 1: Werken als ambtenaar en werken als raadslid is niet met elkaar vergelijkbaar. Daar moet bij de gekozen IT-oplossingen ook rekening mee worden gehouden. Raadsleden werken vooral in de avonduren. Tijdens belangrijke momenten – raadsvergaderingen – is het echt cruciaal dat onze apparatuur goed werkt. Ook werken wij fysiek niet op dezelfde locatie als waar de IT-ondersteuning wordt geboden. Lang niet alle technische problemen kunnen nog op afstand worden opgelost. Antwoord : Een oplossing zou kunnen zijn om 1 of 2 gedeelde laptops in een kast te plaatsen voor als er een laptop stuk gaat of niet werkt? Deze kunnen dan tijdelijk ter vervanging gebruikt worden, mocht dat nodig zijn. Dit wordt verder uitgewerkt in uitvoeringsplan dat in samenwerking tussen de griffie en het team Informatievoorziening wordt opgesteld. Vraag 2: De toegang tot Ibabs mag m.i. nooit worden beperkt tot de beveiligde laptop van de gemeente. Raads- en commissieleden moeten de mogelijkheid hebben om als back-up hun eigen apparatuur te kunnen gebruiken. Dit geldt ook voor bestanden die

		in Teams zijn opgeslagen. Voor e-mail geldt wat mij betreft hetzelfde. Het moet niet zo zijn dat als je laptop kuren heeft, dat je als raadslid dagen niet bij je mail kan tot je naar het gemeentehuis kunt komen. Antwoord: Het is inderdaad ook niet de bedoeling dat de toegang tot iBabs wordt beperkt tot de beveiligde laptop. De applicatie iBabs is een zogenaamde SAAS (Cloud) voorziening die via de meeste internetbrowsers benaderd en gestart kan worden. Onafhankelijk van de ICT-apparatuur. Het kan zelf met een mobiele smartphone. Toegang tot de applicatie iBabs wordt gegeven met het gemeentelijke e-mailaccount als gebruikersnaam, in combinatie met Multifactor Authenticatie (MFA). Dit is op elk ICT-apparaat te gebruiken. Dit geldt ook als het gemeentelijke e-mailadres gebruikt wordt in combinatie met Microsoft Outlook. Voorwaarde is wel dat de Microsoft Authenticator-app op een mobiele telefoon bij de hand is. Eens dat het vervelend is als ICT-apparatuur het niet doet. Dat kan gebeuren, ook met eigen apparatuur. Oplossing zou kunnen zijn om op locatie gedeelde laptops te plaatsen. Vraag 3: De laptops van de gemeente zouden niet 'dichtgezet' moeten zijn, op een manier waarbij voor de installatie van elk programma machtiging nodig is van systeembeheerders of waarbij je niet de juiste toestemmingen hebt om problemen zelf op te lossen. Antwoord: In het geval van zelf applicaties en programma's installeren gaat veiligheid wel boven gebruik. Dit is inderdaad vanuit veiligheidsoverwegingen 'dichtgezet'. Is een programma of applicatie nodig, dan kan deze aangevraagd worden. Deze wordt dan onderzocht, getest en op risico's beoordeeld om vervolgens via het Business portaal beschikbaar gesteld te worden. Het instellen van Wifi netwerken, printers en andere persoonlijk instellingen is gewoon mogelijk. Vraag 4: Er moet zo min mogelijk risico op storingen zijn. Als het niet absoluut noodzakelijk is om gebruik te maken van de werkomgeving van de gemeente, zou ik dat niet willen doorvoeren. Een werkomgeving anders dan de standaard Windows omgeving vergroot de kans dat er IT-ondersteuning nodig is, en het betekent waarschijnlijk ook dat we vastzitten aan het relatief strenge beveiligingsbeleid van de gemeente zelf.

		Antwoord: Storingen kunnen altijd en overal plaatsvinden. Ook met de ‘eigen’ apparatuur. Binnen het gemeentelijke netwerk maken we gebruik van de cloud omgeving van Microsoft. Deze werkomgeving is afgestemd en ingericht op de wensen en eisen vanuit de gemeentelijke organisatie. Daarbij is ook gekeken naar de balans tussen veiligheid en gebruik, op basis van risicoanalyses. Uitgangspunt is dat als er gewerkt wordt met vertrouwelijke informatie en persoonsgegevens, dit veilig gebeurt. Vraag 5: Multifactor authenticatie (MFA) zou niet de dagelijkse praktijk moeten zijn. Het is begrijpelijk dat dit wordt toegepast bij kritieke momenten zoals het instellen van de Outlook-app of voor de eerste keer inloggen op een onbekend apparaat, maar van elke keer weer inloggen met je telefoon wordt niemand vrolijk. Antwoord : Het instellen en gebruiken van MFA is niet specifiek bedoeld om applicaties veilig in te kunnen stellen. Het gaat juist om de informatie en gegevens die in deze applicaties bewerkt en gebruikt wordt. Om de risico’s op incidenten op privacy en informatiebeveiliging te minimaliseren is MFA ingesteld op die applicaties waarin gewerkt wordt met persoonsgegevens en bedrijfsgevoelige informatie. Digitale veiligheid heeft echt prioriteit, maar gebruiksgemak ook. Het idee ontstaat dat het gebruiksgemak er soms een beetje bij inschiet. Voorkomen moet worden dat we straks aan een systeem vastzitten wat meer nadelen dan voordelen heeft. Het feit dat raadsleden niet dagelijks op het gemeentehuis rondlopen maakt het snel krijgen van hulp een stuk lastiger. Antwoord: De balans tussen veiligheid en gebruik is binnen gemeentelijke organisatie ook van groot belang. Hiervoor voeren we risicoanalyses uit op de bedrijfskritische processen en de daarvoor gebruikte ICT-applicaties. Om vervolgens de juiste beslissingen te nemen rekening houdend met deze balans. Vraag 6: Is het mogelijk voor fracties om een afzonderlijk gemeentelijk e-mailadres te krijgen waar alle raads(commissieleden) van die fractie toegang tot hebben? Dus bijvoorbeeld: groenlinkspvda@edam-volendam.nl.

		Antwoord: ja dat is mogelijk.
04-02-2026	PvdA GroenLinks	Vraag 1: Wat is de boekwaarde van de huidige apparatuur die wordt gebruikt door de raads(commissie)leden? Antwoord 1: De afschrijvingstermijn van ICT hardware, zoals Windows laptops, Chromebooks en iPads, is gesteld op 4 jaar. Dat betekent dat de Chromebooks en iPads, die in 2022 zijn afgegeven, een restwaarde hebben van € 0,- Vraag 2: Hoe wordt dit afgeboekt dan wel verrekend in de kosten van het raadsvoorstel? Antwoord 2: Zie antwoord hierboven.
04-02-2026	VVD	Vraag: Wat kost de minimale MS-licentie per jaar die een raadslid doorgaans nodig heeft (om bijv. veilig te kunnen tekstverwerken met Word)? Antwoord: Als gemeentelijke overheid hebben wij met Microsoft een Enterprise overeenkomst gesloten. Daaronder vallen de F3, E3 en E5 licenties. De minimale licentie hierbinnen is een F3 licentie. De jaarlijkse kosten hiervan zijn € 84,-. Binnen een Enterprise omgeving kunnen E3 niet naast een E5 licenties werken. Dus de keuze is of een F3 licentie of een E5 licentie. De mogelijkheden met een F3 licenties zijn natuurlijk veel kleiner. Belangrijkste nadeel in gebruik is dat desktop apps niet gebruikt kunnen worden. Echter met de webversies van MS Word kunnen teksten wel veilig worden verwerkt. Deze webversie bevat de basis functionaliteiten daarvoor. Daarnaast zijn de mogelijkheden op het gebied van informatiebeveiliging ook beperkter.