YOURSAFETYNET

YOURSAFETYNET SCHOOL+ MAKES THE DIFFERENCE IN SECURITY

YOURSAFETYNET SCHOOL+

WHITEPAPER

ACA IT-SOLUTIONS

IS HET ICT- EN PRIVACYBELEID BELEID BINNEN UW SCHOOL AL GOED GEREGELD?

Bescherming persoonsgegevens

Aan de snelheid en de ontwikkeling van de digitale snelweg lijkt geen einde te komen. In tegenstelling tot nog maar enkele jaren terug, rest slechts één druk op de knop om informatie, waaronder persoonsgegevens, in enkele seconden over de gehele wereld te delen of te verspreiden. Deze snelle technologische vooruitgang heeft ook een keerzijde inzake het beschermen van persoonsgegevens. Het is dus niet verwonderlijk dat het ontwikkelen van ICT- en privacybeleid, dat dient ter bescherming van personen binnen de school (zoals medewerkers en leerlingen), vaak achter de feiten aanloopt. Bewustwording is geen overbodige luxe, want uit onderzoek blijkt dat het thema 'ICT beleid' nauwelijks leeft. Ook de landelijke overheden worstelen met dit probleem. Dit blijkt ook uit het feit dat de Europese richtlijn bescherming persoonsgegevens (95/46/EG), sinds 2001 van kracht, nauwelijks op inhoud is gewijzigd.

"Grenzen vervagen waardoor de controle en verwerking van persoonsgegevens toenemen"

Huidige privacywetgeving en datalekken

Tot het moment dat deze EU wetgeving van kracht is hebben we in Nederland de Wet bescherming persoonsgegevens (Wbp). De Autoriteit Persoonsgegevens (AP) waakt over de correcte uitvoering van deze privacywetgeving en is sinds 1 januari 2016 bevoegd om boetes op te leggen bij overtreding van de privacywetgeving. In België is de privacywetgeving ondergebracht in de Wet Verwerking Persoonsgegevens (WVP). De controle, naleving en eventuele sancties vallen onder de verantwoordelijkheid van de Privacycommissie (PC).

De belangrijkste bepalingen uit de privacywetgeving over het rechtmatig omgaan met persoonsgegevens zijn als volgt samen te vatten:

- Persoonsgegevens mogen alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier worden verwerkt.
- Persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. En vervolgens alleen verder worden verwerkt voor doeleinden die daarmee verenigbaar zijn.
- Degene van wie persoonsgegevens worden verwerkt (de betrokkene genoemd), moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt (de zogeheten verantwoordelijke) en van het doel van de gegevensverwerking.
- De gegevensverwerking moeten op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.

AUTORITEIT PERSOONSGEGEVENS

CBPL Commissie voor de bescherming van de persoonlijke levenssfeer

Indien niet aan genoemde criteria wordt voldaan, is dit al een ernstige vorm van datalekken. Een datalek hoeft niet persé veroorzaakt te zijn door een 'technisch' beveiligingsprobleem maar wordt meestal veroorzaakt doordat het interne ICT- en privacybeleid niet op orde is.

Nieuwe Europese privacyregelgeving

De huidige Europese privacyregelgeving 95/96/EG is aan herziening toe. Er zijn voorstellen tot wijziging gepresenteerd, bestaande uit een algemene verordening gegevensbescherming en een richtlijn gegevensbescherming opsporing en vervolging. Op dit moment zijn het Europees Parlement en de Raad van Ministers van de EU begonnen met de bestudering van deze voorstellen. De verwachting is dat deze nieuwe privacyregelgeving dit jaar nog wordt goedgekeurd. Na ratificatie van de landelijke parlementen zal dit de huidige Wet bescherming persoonsgegevens (NL) en de Privacywetgeving (BE) vervangen. YourSafetynet biedt een unieke oplossing met voorbeelddocumenten en procedures die voldoen aan de laatste wet- en regelgeving. De komende wetwijzigingen met (landelijke)amendementen worden via het updatesysteem van YourSafetynet automatisch verwerkt in de geïntegreerde documenten en procedures, waardoor uw organisatie altijd kan worden ingericht volgens de laatste wet- en regelgeving.

"Dankzij YourSafetynet is uw organisatie altijd ingericht volgens de laatste wet- en regelgeving"

Wat is gegevensverwerking?

- De privacywetgeving is van toepassing op alle vormen van het verwerken van persoonsgegevens, ongeacht of die verwerking op papier of in computerbestanden gebeurt.
- Verwerking persoonsgegevens: het hele proces van verkrijgen, combineren, bewerken, ordenen, opslaan, opvragen, doorgeven, vernietigen van gegevens etc. Hieronder vallen ook wachtwoorden en inloggegevens.
- Het geheel of gedeeltelijk geautomatiseerd verwerken van persoonsgegevens moet in principe gemeld worden bij de Autoriteit Persoonsgegevens of de Privacycommissie.

ICT- en privacygedoogbeleid op scholen

Voor zover er beleid is, bestaat bij schoolorganisaties het ICT- en privacybeleid meestal uit 'allerlei puzzelstukjes' die als samenstelling meestal niet aan de criteria van de thans geldende privacywetgeving voldoen. Door allerlei oorzaken of onwetendheid, 'leeft' ICT- en privacybeleid niet echt binnen een schoolorganisatie. Scholen moeten echter wel garant staan voor een veilige leer- en werkomgeving; een onmisbare randvoorwaarde voor goed onderwijs.

Uit een onderzoek[1] onder ruim 20.000 ouders en leerlingen, blijkt dat scholen bescherming zouden moeten bieden bij het gebruik van (online) media. Leerlingen hebben recht op veilige media, bescherming tegen schadelijke beelden/teksten en online privacy. De uitvoering van dit recht begint met het maken van goede afspraken, waarin een belangrijke rol is weggelegd voor het bestuur, directie en ICT beheer: Hoe bescherm ik de leerlingen, leerkrachten en de school tegen ongewenst internetgebruik en misbruik van de privacy?

Voor iedere schoolorganisatie geldt: is er een ICT- en privacybeleid waarin duidelijke afspraken zijn vastgelegd tussen het schoolbestuur, directie, leerkrachten, leerlingen en uiteraard de ouders? Wat is er geregeld, zonder dat leerkrachten en leerlingen het gevoel krijgen gecontroleerd of betrapt te worden? Worden bepaalde websites gefilterd tegen schadelijke beelden en teksten? Welke persoonsgegevens worden bewaard en hoe lang? Wat zijn de spelregels inzake sociale media? Hoe wordt omgegaan met o.a. loggen, verwerken en rapporteren van persoonsgegevens? Wordt de privacywetgeving wel gerespecteerd? Kortom: eenvoudige vragen waarop men binnen de schoolorganisatie meestal geen eenduidig antwoord heeft.

Hierdoor komen scholen steeds vaker in juridisch 'conflict' met het bestaande ICT gedoogbeleid (lees: door het ontbreken van strategisch beleid). Het gevolg is dat leerkrachten, leerlingen en de school niet of nauwelijks beschermd worden tegen inbreuk op de privacy. Daardoor zijn zij min of meer 'vogelvrij' zijn wanneer het gaat over het verwerken en rapporteren van persoonlijke gegevens.

"De media-aandacht omtrent datalekken zet schoolorganisaties weer op scherp"

ICT- en privacybeleid op school, waarom gaat het mis?

- Laag op de prioriteitenlijst, leeft niet echt.
- Juridische en technische complexiteit.
- Steeds wijzigende regel- en wetgeving.
- Ingewikkelde procedures en handelingen.
- Onwetendheid, ICT- en privacybeleid ontbreekt, is verouderd en/of niet bekend
- Wie is de strategisch 'verantwoordelijke'?
- Onbekendheid welke persoonsgegevens mogen/moeten worden verwerkt, bijvoorbeeld in leerling/personeelsdossiers

1. *Mediawijzer.net*

of leerlingen volg systeem (LVS).
- Persoonsgegevens worden verstrekt aan derden zonder toestemming van betrokkenen of zonder deugdelijke bewerkersovereenkomsten.
- Geen inventarisatie waar persoonsgegevens staan en verwerkt worden? Onduidelijk wie toegang hebben tot persoonsgegevens.
- Wel 'beleid', maar niet getoetst aan de huidige regel- en wetgeving.
- Ontbreken ICT-gebruiksreglement, privacyreglement, reglement sociale media, etc.
- Geen beleid ten aanzien Wi-Fi (toegang) of BYOD.
- Onwetendheid over juridische risico's naar:
  - Leerkrachten, medewerkers, leerlingen en ouders/ verzorgers.
  - Sociale partners (OR, Medezeggenschapsraad, etc.).
  - Autoriteit Persoonsgegevens (AP) of Privacycommissie (PC).
  - Business Software Alliance (BSA) inzake het gebruik van illegale software.

Wijziging privacywetgeving

Na het 'vermeende' datalekken binnen het onderwijs heeft de overheid haast gemaakt met het wijzigen van de privacywetgeving die per 1 januari 2016 in werking is getreden. Deze wetswijziging heeft verregaande consequenties voor schoolorganisaties, bestuurders en ICT beheerders. De wet beschermt leerkrachten, leerlingen en de schoolorganisatie o.a. tegen datalekken bij diefstal, verlies of misbruik van persoonsgegevens. Daarnaast mag het loggen, verwerken en rapporteren van persoonsgegevens, waaronder ook het internet- en computergebruik, niet zonder redenen naar personen leiden. Ook ICT -en privacyreglementen voor leerkrachten en leerlingen moeten, als onderdeel van het allesomvattend ICT beleid, aan wettelijke criteria en procedures te voldoen. Bij inbreuk op de privacy, die de persoonlijke levenssfeer van de betrokken leerkrachten, leerlingen of organisatie aantast, moet dit onmiddellijk aan de autoriteit gemeld worden. Iedereen moet erop kunnen vertrouwen dat zijn persoonsgegevens voldoende wordt beveiligd. Slechte beveiliging kan leiden tot een datalek en vervolgens tot misbruik van deze gegevens.

Wanneer heeft een school ook een meldplicht?

Een schoolorganisatie is verplicht een datalek te melden indien er risico's voor betrokkenen dreigen. Deze meldplicht geldt aan de desbetreffende controlerende instantie en naar de betrokkene(n) wanneer er sprake is van:

- Verwerking van persoonsgegevens zonder legitiem belang.
- Het gebruiken van persoonsgegevens voor onverenigbare doeleinden.
- Het overtreden van het verbod inzake het verwerken van bijzondere gegevens.
- Het zich niet houden aan de regels rondom data export naar niet Europese landen.
- Onvoldoende informatieverstrekking naar betrokkenen over het privacy beleid van de school.
- Verwerken (grensoverschrijdend) internetgebruik waarbij de juiste procedures ontbreken.
- Niet geaccrediteerde bewerkers waaronder de ICT coördinator en ICT beheerder (derden).

Wat kunnen additionele gevolgen zijn van ontbreken van ICT- en privacybeleid?

- Imago- en reputatieschade van de schoolorganisatie in geval van datalekken.
- Risico van instabiel ICT netwerk door onbeperkt gebruik van bandbreedte, privé applicaties, logs, data, etc.
- Ongeorganiseerd BYOD gebruik verhoogd het risico op o.a. spam, malware, computervirussen en gebruik van illegale software.
- Ontbreken ICT- en privacybeleid geeft juridische beperkingen op corrigerend ingrijpen.
- Bij gebruik van illegale software, aansprakelijkheidstelling door de BSA.

Is encryptie de oplossing ter voorkoming van datalekken?

Het is een grote misvatting dat encryptie van datastromen 'de oplossing' is ter voorkoming van datalekken. Door encryptie kan data veilig worden uitgewisseld tussen personen over een onveilig communicatiekanaal, met andere woorden waar ook derden toegang kunnen hebben, zoals het internet. Voordat encryptie van data aan de orde is, dient er duidelijkheid te zijn omtrent de autorisatie van het databewerker. Is de ICT coördinator of de ICT bewerker (vaak extern) geaccrediteerd of bevoegd om de data te beoordelen, te loggen, te verwerken, te rapporteren, etc.? Is de data rechtmatig verzameld en met instemming van leerkrachten, leerlingen en organisatie? Zijn de juiste reglementen en procedures gehanteerd voor het verzamelen van deze gegevens?

Indien de autorisatie en voorwaarden ontbreken waarop de ICT coördinator of ICT bewerker toegang tot bestanden en datastromen hebben, dan is dit op zich al een ernstige vorm van datalekken. In de praktijk kan dus onrechtmatig verkregen

persoonsinformatie voorzien zijn van encryptie! Bovendien is datalekken niet beperkt tot uitsluitend digitale datastromen, want dit geldt nadrukkelijk ook voor verwerking van persoonsgegevens op alle papier- en documentenstromen.

"Encryptie en een bewerkersovereenkomst zijn slechts onderdelen van de verplichte privacywetgeving"

Boetebevoegdheid van de Autoriteit Persoonsgegevens (NL) en de Privacycommissie (BE)

De Autoriteit Persoonsgegevens (NL) en de Privacycommissie (BE) hebben de bevoegdheid om bij overtreding hoge boetes op te leggen. Bij grove nalatigheid (lees: niets gedaan ter voorkoming van datalekken) kan de schoolorganisatie direct worden beboet. Daarnaast geldt ook het risico van bestuurlijke aansprakelijkheid. In Nederland bedragen de boetes maximaal € 820.000,00 (bij klasse III); in België ligt een wetsontwerp om de boete te verhogen tot maar liefst € 20 miljoen. Boetes zijn van toepassing indien:

- Datalekken niet wordt gemeld.
- Persoonsgegevens niet op een behoorlijke of zorgvuldige manier zijn verwerkt, langer worden bewaard dan noodzakelijk, de beveiliging niet deugt, het beheer van persoonsgegevens slecht is georganiseerd of gevoelige informatie is misbruikt, etc.
- Verwerking van persoonsgegevens niet is gemeld bij de Autoriteit Persoonsgegevens of Privacycommissie.

"Bij overtreding kunnen aan schoolorganisaties boetes worden opgelegd tot maar liefst €820.000,00"

Wat betekent de privacywetgeving voor een schoolorganisatie?

Beveiliging van persoonsgegevens moet binnen een schoolorganisatie een speerpunt van aandacht zijn. Om datalekken te voorkomen moeten scholen, bedrijven en overheden, die persoonsgegevens gebruiken, passende technische en organisatorische maatregelen treffen. De basis van deze maatregelen ligt in de ontwikkeling van een alles omvattend ICT beleid onder het gezag van de 'verantwoordelijke'. Het gaat hierbij vooral om het gegeven hoe een schoolorganisatie omgaat met persoonsgegevens. Een meldplicht kan bijvoorbeeld al aan de orde zijn wanneer een (arbeidsrechtelijk) geschil over ICT gebruik is ontstaan tussen schoolorganisatie en leerkracht of leerling. Het oorzakelijk verband, de controle en verwerking van dergelijke geschillen moeten altijd gemeld worden aan de Autoriteit Persoonsgegevens of Privacycommissie. Vervolgens zal men oordelen of er sprake is van verwerking persoonsgegevens en voldaan is aan de wettelijke criteria inzake de privacywetgeving. Schoolorganisaties waarbij het geldende ICT- en privacybeleid niet voldoet aan de privacywetgeving krijgen bij nalatigheid onmiddellijk een boete opgelegd. Bestuurders, directies en ICT beheerders kunnen deze wet niet langer negeren en staan daarom voor de volgende strategische vraagstukken:

1. **Willen we ICT- en privacybeleid?**
2. **Dient dit beleid aan de privacywetgeving te voldoen?**
3. **Voldoet ons ICT- en privacybeleid (voor zover dat er is) aan de privacywetgeving?**

ICT- en privacybeleid ingericht volgens de privacywetgeving is een vrij complexe materie. Het antwoord op de laatste vraag is meestal: weet het niet of nee.

Wat is ICT- en privacybeleid?

Dit zijn afspraken en beleidsdocumenten over:

- Gebruik van hardware, software, mobiele devices, etc.
- Monitoren, loggen, registreren, verwerken, rapporteren, etc.
- Criteria om met de BYOD toegang tot het schoolnetwerk te krijgen.
- Autorisatie, accreditering, geheimhouding, etc.
- Filteren, blokkeren, regulieren, etc.
- Rechtmatige bewaarperiode opgeslagen loggegevens.
- Privacyreglementen.
- ICT-gebruiksreglementen.
- Gebruik van sociale media.
- Gebruik van beeldmateriaal.
- Privé internetgebruik onder school/werktijd.
- Procedures en handelingen om aan wettelijke criteria te voldoen.

De ontwikkeling, handhaving en controle moet voldoen aan de privacywetgeving.

Privacywetgeving: kansen voor leerkrachten, leerlingen en schoolorganisaties!

De verplichte privacywetgeving biedt scholen, leerkrachten en leerlingen het legitieme recht om afstand te nemen van het bestaande risicovolle ICT-gedoogbeleid. ICT beleid wat aan de privacywetgeving voldoet geeft kansen aan leerkrachten en leerlingen.

Leerkrachten en leerlingen hoeven niet langer het gevoel te hebben onterecht gecontroleerd of betrapt te worden tijdens het internet- of computergebruik of dat persoonsgegevens ten onrechte worden verwerkt. Strategisch ICT- en privacybeleid geeft scholen de noodzakelijke prikkel voor een bewustere en verantwoorde omgang met persoonsgegevens. Het is een welkome kans voor een positieve profilering richting de buitenwereld en het op orde brengen van interne ICT processen en procedures. Tot slot biedt ICT beleid dat voldoet aan de wettelijke procedures en regels bescherming voor alle partijen binnen een juridisch kader, met als doel:

- Beschermen persoonsgegevens en financiële informatie.
- Voorkomen van datalekken.
- Voorkomen van aansprakelijkheden en boetes.

"Duidelijkheid schept (arbeids)vreugde en voorkomt aansprakelijkheid"

ICT- en privacybeleid op school, enkele begrippen!

Enkele termen en begrippen uit de Privacywetgeving:

Verantwoordelijke:

- De verantwoordelijke stelt doel en middelen vast van de verwerking van persoonsgegevens. Dit is meestal directie of bestuur.
- De verantwoordelijke moet toezien op de naleving van de Privacywetgeving.
- De verantwoordelijke heeft de verantwoordelijkheid ervoor te zorgen dat de bewerker maatmaatregelen treft die nodig zijn om aan de meldplicht voor datalekken te kunnen voldoen.

Bewerker (NL) of Verwerker (BE):

- De bewerker is degene die de verwerking van persoonsgegevens uitvoert (in opdracht van de verantwoordelijke).
- Een interne bewerker is iemand die meestal direct onder het gezag van de verantwoordelijke valt. Dit kan bijvoorbeeld een interne ICT medewerker zijn.
- Een externe bewerker is iemand die de verwerking uitvoert, zonder aan rechtstreeks gezag van de verantwoordelijke te zijn onderworpen. Dit kan bijvoorbeeld een externe ICT dienstverlener zijn.
- De bewerker heeft géén wettelijke meldplicht, tenzij het over persoonsgegevens gaat waar hij als verantwoordelijke het gezag over heeft.
- Maar ...in veel gevallen is de bewerker wel de eerste die kennis krijgt van een opgetreden datalek!

Inventariseer waar persoonsgegevens zich bevinden of worden verwerkt, welke gegevens worden verwerkt en van wie (medewerkers, leerlingen, derden, etc.). Onderscheid de belangrijkste rollen en verantwoordelijkheden, zowel intern als extern. Formuleer ICT- en privacybeleid met instemming van de medezeggenschapsraad, ouderraad en voer dit beleid uit d.m.v. protocollering, procedures en reglementen.

HOE MAAKT YOURSAFETYNET SCHOOL+ HET VERSCHIL?

YourSafetynet school+ is een unieke software oplossing waarmee de 'verantwoordelijke' en de 'bewerker' van de school actief ondersteund worden met de ontwikkeling, handhaving en controle inzake de ICT- en privacywetgeving. Via het menu zijn interactieve wizards beschikbaar voor ICT-beleid, privacybeleid en anti-pestbeleid. De gebruiker wordt met behulp van de unieke wizard met duidelijke vragen, stap voor stap door het proces geleid. Bij iedere vraag verschijnt bovendien een uitgebreide toelichting. Op basis van het gekozen antwoord worden automatisch de juiste documenten, procedures en reglementen beschikbaar gesteld. Binnen de wizard worden ook actieve tips en suggesties gegeven ter voorkoming van datalekken en onrechtmatig verwerken. Mocht er tijdens het beheer van het beleid een selectie worden gemaakt die mogelijk in strijd is met de privacywetgeving dan verschijnt er een pop-up waarschuwing met een advies.

De uitvoering van ICT- en privacybeleid start met een stappenplan. Om een allesomvattend beleid binnen een organisatie uit te rollen, begint het met het maken van duidelijke afspraken, reglementen en procedures waarvan de inhoud en werkwijze moet voldoen aan de thans geldende wetgeving. Ook de technische uitvoering van de software moet aan een aantal voorwaarden voldoen. ICT-beleid wordt vaak ten onrechte alleen gelijk gesteld aan het filteren of bokkeren van bepaalde websites. YourSafetynet school+ gaat verder en biedt hulp bij het handhaven van het totale beleid, door controle en ingrijpen bij ongewenst internetgedrag, volgens de geldende wetgeving.

Uiteraard voldoet YourSafetynet school+ aan huidige strenge privacywetgeving van:

- België: Wet Verwerking Persoonsgegevens (WVP)
- Nederland: Wet bescherming persoonsgegevens (Wbp)

"Nog nooit was uitvoering van verplichte wetgeving zo eenvoudig"

HET STAPPENPLAN VAN YOURSAFETYNET

Stap 1: Ontwikkeling van beleid

In deze fase wordt de selectie gemaakt uit ICT-beleid, privacybeleid of anti-pestbeleid. Voor ieder type beleid zijn er interactieve wizards, procedures en voorbeelddocumenten (templates) beschikbaar. Het gaat onder andere om:

- Wizard invoering ICT-beleid
- Wizard uitvoering privacybeleid
- Wizard invoering Anti-pestbeleid
- ICT gebruiksreglementen voor leerlingen en medewerkers
- Reglementen gebruik Sociale media
- Privacyreglementen voor leerlingen en medewerkers
- Bewerkersovereenkomsten intern en extern beheer
- Vrijwaringsovereenkomsten
- Procedures melding datalekken
- Toestemming gebruik beeldmateriaal
- En meer

"De wizards leiden stap voor stap door het proces"

Stap 2: Handhaving van beleid

Het geselecteerde beleid is alleen uitvoerbaar en te handhaven door:

- Besluitvorming van en met de strategisch 'verantwoordelijke'.
- Expliciete toestemming tot uitvoering bestuur, directie, medezeggenschapsraad, ouderraad en/of leerlingen.
- Ondertekening van de afspraken door de belanghebbenden en de vertegenwoordigers van de belanghebbenden.
- Het gebruik van de beschikbaar gestelde documenten en procedures.
- Het volgen van de juiste procedures en handelingen.
- Het gebruik van de geïntegreerde ICT-gebruiksreglementen, privacyreglementen en reglementen voor sociale media, die aan de wetgeving voldoen.
- Beleid voor BYOD en het voorkomen van aansprakelijkheid naar de BSA inzake het gebruik van illegale software.
- Het beleid en bijbehorende documenten periodiek te toetsen aan eventuele wetswijzigingen. YourSafetynet voorziet in automatische updates, waardoor de voorbeelddocumenten, procedures en reglementen altijd up-to-date zijn en voldoen aan de laatste wetgeving.

De handhaving, of zelfs het afdwingen, van het geselecteerde beleid kan actief bekrachtigd worden via YourSafetynet school+:

- Voordat men met de computer of mobile devices toegang krijgt tot het netwerk van de school dient men via een pop-up akkoord te gaan met het geldende ICT- en privacybeleid.
- Vervolgens worden, bij akkoord van de gebruiker, de unieke gegevens zoals account, MAC adres en datum geregistreerd.
- Uiteraard kunnen aan deze beleidsdocumenten andere documenten worden gekoppeld zoals het leerlingenstatuut of huishoudelijk reglement.
- Wanneer gebruikers het geldende ICT-beleid negeren door dingen te doen die niet zijn toegestaan, dan wordt dit door de software geregistreerd of geblokkeerd (afhankelijk van de instellingen).
- Filtering van niet toegestane websites, zoals porno, gokken, geweld, discriminatie, etc.
- Regulering: wanneer, en hoe lang, worden bepaalde software of websites toegestaan? Bijvoorbeeld reguleren van sociale media; wel toegestaan tijdens de pauzes maar niet (of beperkt) tijdens de lessen.
- Actieve controle of blokkeren op het gebruik van datadragers (USB/SD) ter voorkoming onrechtmatig downloaden van schoolbestanden.
- Screenshot Alarmknop, de grootste preventie in de strijd tegen het cyberpesten op school.
- Instellingen kunnen onafhankelijk van elkaar gemaakt worden op organisatie-, school-, klas- of gebruikersniveau.

"Beleid is alleen verdedigbaar door juiste procedures en bewaking"

Stap 3: Controle en monitoren beleid

Controle is de meest preventieve maatregel ter voorkoming van misbruik inzake het ICT gebruik. Tevens beschermt het bij handhaving van de privacywetgeving op school.

- Loggen, verwerken en rapporteren van internet- en computergebruik, waaronder gebruikte software, bezochte of geblokkeerde websites, pestdetectie, opslag USB/SD verkeer, etc.
- De rapportage en statistieken geven inzichten in de aantallen, duur, tijdstip, periode en datum.
- Via het dashboard snel inzichtelijke verbanden tussen scholen, klassen of leerlingen/leerkrachten, dus efficiënt organiseren.
- Rapportage is direct beschikbaar op organisatie, school en klas niveau.
- Controle op individuele personen (lees: overtreders) doordat de juiste procedures zijn gevolgd.
- Automatische verversing van data waardoor altijd actuele informatie beschikbaar is.
- Indien tijdens het beheer handelingen worden verricht of instellingen worden gemaakt die mogelijk in strijd zijn met de privacywetgeving verschijnen pop-up waarschuwingen met toelichting en advies.
- Opgeslagen loggegevens worden automatisch vernietigd nadat de wettelijk maximale bewaarperiode (volgens de wetgeving) is overschreden. De wet spreekt hier bovendien over een weggooi-verplichting in plaats van over een bewaarperiode.

"Slechts 3 stappen voorkomen onrechtmatig verwerken van persoonsgegevens en datalekken"

Anti-pestbeleid

Naast het ICT- en privacybeleid voorziet YourSafetynet in procedures om een anti-pestbeleid op school in te voeren. Op scholen met een duidelijk anti-pestbeleid worden leerlingen duidelijk minder gepest. Om pestgedrag blijvend te verminderen moeten scholen, samen met de leerlingen, ouders en leerkrachten, de aandacht voor het anti-pestbeleid blijven vasthouden. De overheid pleit voor meer preventie en heeft inmiddels plannen om het pesten op scholen hard aan te pakken.

Binnen YourSafetynet school+ kan via een unieke wizard een anti-pestbeleid worden geïmplementeerd. Dit anti-pestbeleid is voorzien van duidelijke implementatie- en instructieprocedures, waaronder de doeltreffende vijfsporenaanpak. De uitvoeringsvorm voldoet aan het plan van aanpak conform de adviesregels Nationaal Onderwijsprotocol tegen pesten. Mocht het dan toch een keertje misgaan, dan kunnen leerlingen de screenshot alarmknop van YourSafetynet school+ gebruiken, waarmee een schermafbeelding gemaakt wordt van bijvoorbeeld bedreigende teksten, websites, beelden via Facebook, Skype, etc. Deze schermafbeeldingen kunnen als bewijsvoering worden overlegd.

"Ook rapportages binnen het anti-pestbeleid dienen aan de privacywetgeving te voldoen"

YOURSAFETYNET PLATFORM

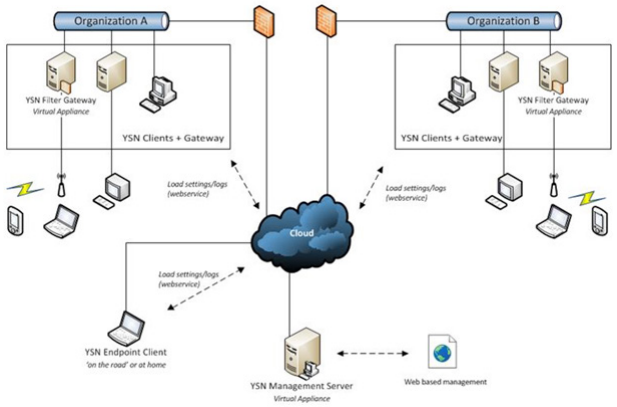
Dankzij het web-based multi-user beheerplatform is YourSafetynet school+, in verhouding tot de gemiddelde firewall of UTM oplossing, zeer eenvoudig in gebruik en beheer. Naast de ICT beheerder (manager die toegang heeft tot alle scholen binnen de organisatie), kan een ICT-coördinator van een specifieke school zelf de instellingen maken dan wel wijzigen.

De volgende ICT hiërarchie is daardoor uitvoerbaar:

- Masterniveau: Overkoepelende ICT manager (alle scholen of locaties)
- Organisatieniveau: ICT coördinator (school of locatie)
- Profielniveau: Leerkracht (groep/klas)

YourSafetynet school+ bestaat uit drie onderdelen:

- Management Server [virtual appliance]
- Endpoint Client [msi pakket, optioneel]
- Filter Gateway [virtual appliance, optioneel]



Voorbeeld deployment YourSafetynet platform (grote versie op volgende pagina)

Management Server

Dit is het hoofdonderdeel van YourSafetynet. Deze server in de vorm van een virtual appliance biedt een web interface (https) voor het beheer van vrijwel alle instellingen binnen YourSafetynet. Het is het centrale punt voor alle instellingen, logs, statistieken en rapporten.

Met de YourSafetynet Management server beheert u instellingen en gegevens van meerdere organisaties op één centraal punt. Het beheer wordt gedaan door één of meer Managers. Er kunnen een onbeperkt aantal verschillende managers aangemaakt worden (eventueel met afwijkende rechten).

Voor de daadwerkelijke filtering en handhaving van uw ICT beleid, moeten er Filter Nodes gekoppeld worden aan de Management Server. Dit kunnen Endpoint Clients en/of Filter Gateways zijn. De Management Server stuurt instellingen door naar de Filter Nodes en ontvangt eventuele logs over bijvoorbeeld bezochte website of gebruikte software. Deze communicatie verloopt over beveiligde (HTTPS) verbindingen.

Endpoint Client

Dit is een software pakket voor Windows machines en terminal servers (te installeren via een msi pakket). Dit pakket installeert zichzelf als een lokaal filter op de computer. Alle filtering vindt lokaal plaats op de computer.

Naast een internetfilter heeft de endpoint client nog extra filter mogelijkheden op het gebied van software (reguleren van gebruik van software).

Daarnaast biedt het een 'screenshot alarm knop' waarmee de gebruiker direct een screenshot kan maken. Deze wordt doorgestuurd naar de Management Server en is daar door de managers te bekijken. Deze alarmknop is vooral handig bij technische problemen of als er sprake is van pestgedrag. De Endpoint Client zal instellingen en logs uitwisselen met de Management server (over HTTPS).

Filter Gateway

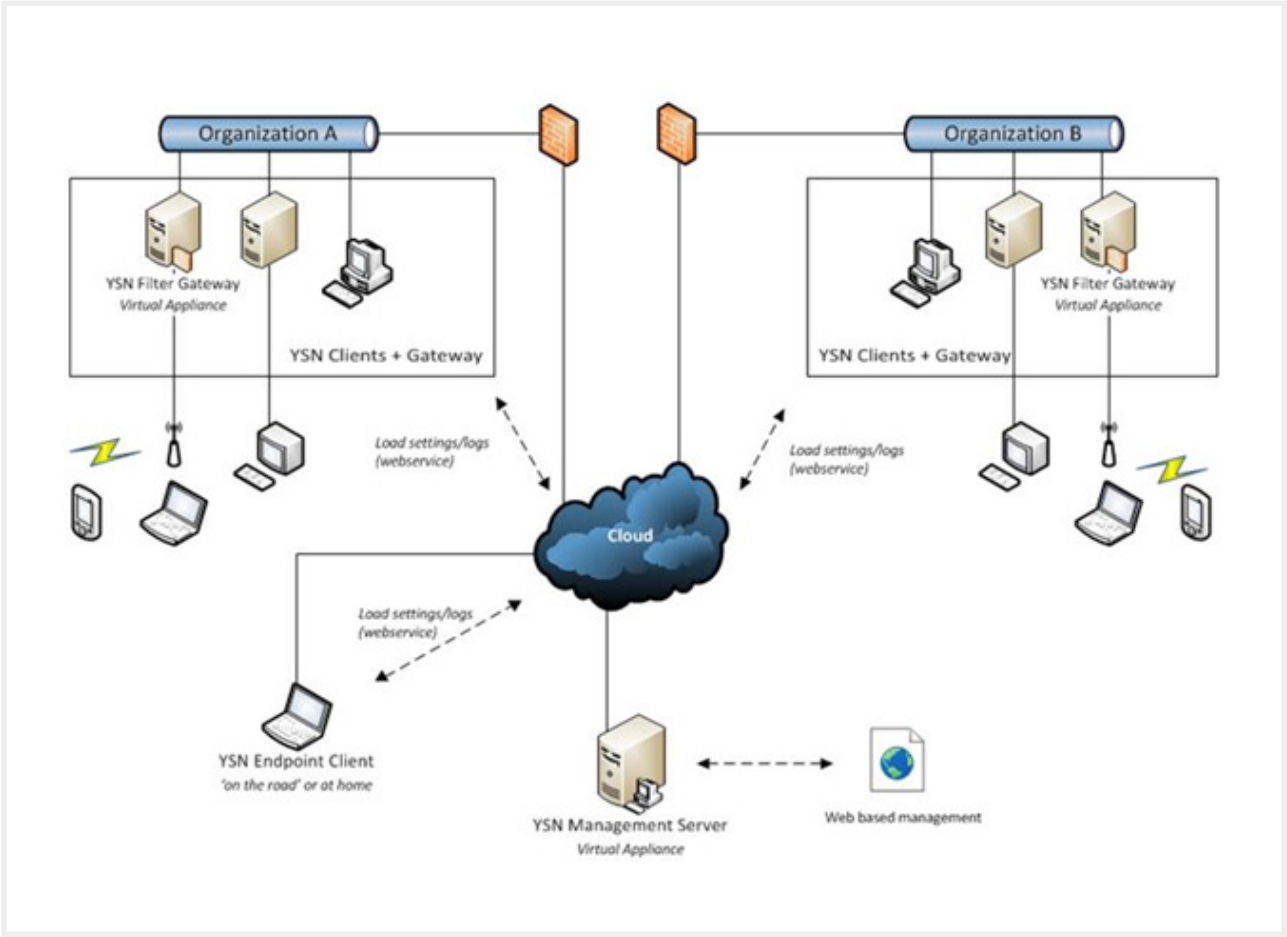
Dit is een intermediate gateway in de vorm van een virtual appliance. Dit onderdeel biedt de mogelijkheid om computers, laptops, mobiele devices te filteren zonder dat daar software voor geïnstalleerd hoeft te worden.

De Filter Gateway is een Captive Portal; een soort firewall, maar dan binnen uw netwerk. Het 'vangt' al het binnenkomende netwerkverkeer af en filtert dit volgens de ingestelde beperkingen. De eerste keer dat een gebruiker verbinding probeert te maken zal de gateway de gebruiker doorsturen naar een inlogformulier. Hier moet de gebruiker inloggen (met zijn Active Directory of LDAP credentials) en moet dan eventueel nog akkoord gaan met het ICT gebruiksreglement dat u heeft ingesteld. Daarna kan de gebruiker verder surfen (binnen de beperkingen van de ingestelde filters).

Een Filter Gateway appliance zal instellingen en logs uitwisselen met de Management Server (over HTTPS).

VOORBEELD DEPLOYMENT YOURSAFETYNET PLATFORM

Dankzij het web-based multi-user beheerplatform is YourSafetynet school+, in verhouding tot de gemiddelde firewall of UTM oplossing, zeer eenvoudig in gebruik en beheer. Naast de ICT beheerder (manager die toegang heeft tot alle scholen binnen de organisatie), kan een ICT-coördinator van een specifieke school zelf de instellingen maken dan wel wijzigen.



Voorbeeld deployment YourSafetynet platform

YOURSAFETYNET

YOURSAFETYNET SCHOOL+

Meer informatie
Wilt u meer informatie of een afspraak maken? Neemt u dan contact met ons op via onderstaande contactgegevens.

ACA IT-Solutions
Beemdstraat 38
Postbus 7070
5605 JB EINDHOVEN

T +31 (0)40 – 8 800 100
E info@aca-it.nl
I www.aca-it.nl

A·C·A IT-SOLUTIONS

On Premise
ICT OP LOCATIE

Cloud Solutions
WERKEN IN DE CLOUD

IT Services
DIENSTEN & SUPPORT