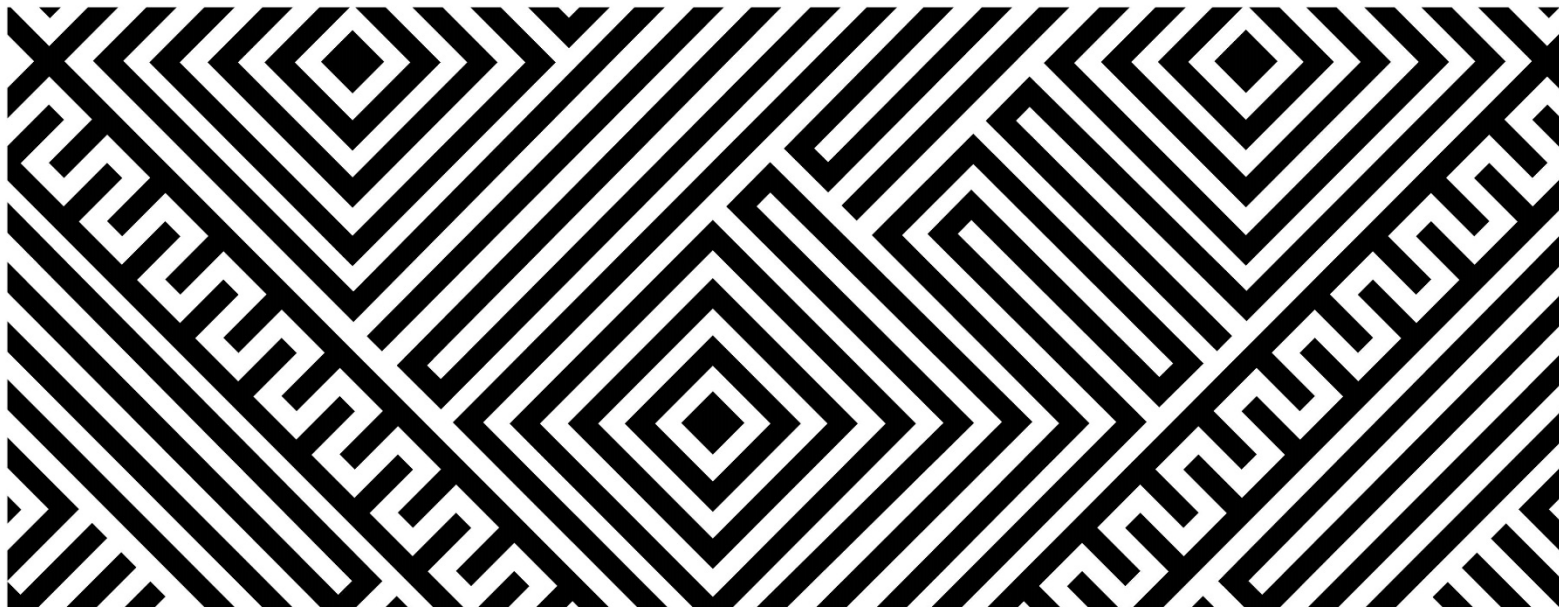


Richtlijn verantwoord digitaal werken

Medewerkers en gasten



Versiebeheer

Versie	Status	Datum	Auteur	Omschrijving
1.0	Ter goedkeuring	23-11-2020	Nancy Strijbos, Erwin Huggers	Ter goedkeuring aangeboden

Vastgesteld door SintLucas:

Versie	Datum	Naam/gremium	Functie
1.0	07-12-2020	MT	-
1.0	21-01-2021	OR	-

Inhoud

1	Inleiding	4
1.1	Doel van deze richtlijn	4
1.2	Toepassingsgebied en gebruiker	4
1.3	Begrippenverklaring	4
2	Informatiebeveiliging en Privacy (AVG)	5
2.1	Wat verstaan we onder privacy?	5
2.2	Hoe gaan we binnen SintLucas om met informatiebeveiliging en privacy?	5
3	Gebruiksrichtlijnen	5
3.1	Omgaan met (bijzondere) persoonsgegevens en vertrouwelijke informatie	5
3.2	Hoe te handelen bij een (vermeend) datalek	5
3.3	Bewaartermijnen	5
3.4	Omgaan met intellectueel eigendom	6
3.5	Online samenwerken: bestanden delen	6
3.6	Online samenwerken: omgaan met e-mail	6
3.7	Online samenwerken: vergaderen	6
3.8	Omgaan met internet	6
3.9	Gebruik van social media	7
3.10	Ongewenst gebruik algemeen	7
4	Gebruik middelen en faciliteiten	7
4.1	Toegang ICT-faciliteiten	7
4.2	Gebruikersnaam en wachtwoord	7
4.3	Gebruik ICT-faciliteiten	8
4.4	Veilig thuiswerken	8
4.5	Omgaan met hardware en software	8
4.6	Opslaan van informatie	9
5	Toezicht, controle, klachten en maatregelen	9
5.1	Recht op toezicht en controle	9
5.2	Periodieke rapportages	9
5.3	Klachten	10
5.4	Rechtspositionele maatregelen	10
6	Overige bepalingen	10
7	Bijlage 1 Verwijzingen en links	11
7.1	Documenten	11
7.2	Overige verwijzingen:	11
7.3	Toelichting Auteurswet en auteursrecht in het onderwijs	11

1 Inleiding

SintLucas streeft ernaar een veilige omgeving in te richten voor haar medewerkers, studenten en leerlingen. Als gebruiker van diverse ICT-faciliteiten is het van belang dat je weet hoe je hier zorgvuldig mee omgaat. Aan alle ICT-faciliteiten en middelen, zoals internet, e-mail, laptops en smartphones zitten zowel voordelen als risico's. SintLucas zorgt voor een veilige ICT-omgeving. In deze richtlijn lees je wat we van jou als gebruiker verwachten.

1.1 Doel van deze richtlijn

In deze richtlijn geeft het College van Bestuur aan wat haar beleid is ten aanzien van het gebruik van ICT-faciliteiten, beschikbaar gesteld door SintLucas aan de gebruiker. Het instellen van deze richtlijn heeft tot doel de regels en voorwaarden voor het gebruik van ICT-faciliteiten, inclusief de wederzijdse rechten en plichten van de werkgever en de werknemer, bekend te maken.

1.2 Toepassingsgebied en gebruiker

Deze richtlijn is van toepassing op het gebruik van alle huidige en toekomstige ICT-faciliteiten en/of middelen die SintLucas aan haar gebruikers ter beschikking stelt. Bij gebruik van eigen faciliteiten en/of middelen voor SintLucas-doeleinden gelden dezelfde regels en voorwaarden.

Deze richtlijn geldt voor alle gebruikers van SintLucas. Onder gebruikers verstaan wij in dit kader:

- Personen met een arbeidsovereenkomst (inclusief vakantiekrachten)
- Leden Raad van Toezicht
- Vrijwilligers
- Stagiairs
- Ingeleende personen, zoals gastdocenten en zzp'ers
- Gastgebruikers, personen van andere organisaties die gebruik maken van de faciliteiten, infrastructuur of ICT-middelen van SintLucas

1.3 Begrippenverklaring

In deze richtlijn worden de volgende begrippen gehanteerd (op alfabetische volgorde)

- Functionaris voor Gegevensbescherming (FG-er): houdt binnen de organisatie toezicht op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG).
- Gebruiker: degene die gebruik maakt van de ICT-faciliteiten van SintLucas.
- Hoax: een waarschuwing die per e-mail of via sociale netwerken wordt verspreid. Deze informatie is niet waar, maar wordt wel als zodanig gepresenteerd. Je wordt gevraagd het bericht met zo veel mogelijk mensen te delen.
- IBP-beleid: Informatiebeveiligings- en privacybeleid
- ICT: informatie- en communicatietechnologie
- ICT-faciliteiten en -middelen: alle hulpmiddelen die worden gebruikt voor de geautomatiseerde informatievoorziening, zoals apparatuur, programmatuur, netwerken, internet en e-mail.
- Manager Informatievoorziening: houdt toezicht op het functioneren van de ICT-faciliteiten van SintLucas.
- Op locatie (werkplek): de plaats waar het gebruik van de ICT-faciliteiten plaatsvindt, inclusief de apparatuur die hiervan onderdeel uitmaakt.
- Phishing: poging van criminelen om geld of gegevens te stelen via berichten die gekoppeld zijn aan gelijkende, maar valse websites.

2 Informatiebeveiliging en Privacy (AVG)

2.1 Wat verstaan we onder privacy?

Het onderwijs is in toenemende mate afhankelijk van informatie in combinatie met ICT. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord om te gaan met persoonsgegevens. Persoonsgegevens moeten verwerkt worden volgens de huidige wet- en regelgeving. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijk persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. Denk hierbij bijvoorbeeld aan het verzamelen, bewaren, raadplegen, verspreiden en vernietigen van gegevens.

2.2 Hoe gaan we binnen SintLucas om met informatiebeveiliging en privacy?

Het Informatiebeveiligings- en privacybeleid (IBP) van SintLucas (zie bijlage 1, Documenten) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans is tussen privacy, functionaliteit en veiligheid. Het uitgangspunt hierbij is dat de persoonlijke levenssfeer van de betrokkene (onder andere medewerkers, studenten/leerlingen en hun ouders/verzorgers) wordt gerespecteerd en dat SintLucas voldoet aan relevante wet- en regelgeving. Deze richtlijn komt voort uit het IBP-beleid.

De belangrijkste bepalingen uit de AVG zijn (kort samengevat):

- Persoonsgegevens mag je alleen verwerken in overeenstemming met de wet. Voor de betrokkene (dat is degene van wie de persoonsgegevens verwerkt worden) moet het duidelijk en transparant zijn hoe en waarom de persoonsgegevens verwerkt worden.
- Het verzamelen van persoonsgegevens mag alleen met een gerechtvaardigd doel. Dit doel moet welbepaald zijn en vooraf uitdrukkelijk worden omschreven.
- De persoon van wie de persoonsgegevens worden verwerkt moet in elk geval op de hoogte zijn van de organisatie of persoon die deze gegevens verwerkt en het doel van deze gegevensverwerking.
- Het uitgangspunt is: verwerk 'zo min mogelijk' gegevens. Zorg dat wat je verwerkt juist is en regelmatig wordt geactualiseerd.

SintLucas heeft een Functionaris voor Gegevensbescherming (FG-er) aangesteld om de rechten van éénieder te waarborgen.

3 Gebruiksrichtlijnen

3.1 Omgaan met (bijzondere) persoonsgegevens en vertrouwelijke informatie

Vanuit je functie of rol kun je toegang hebben tot privacygevoelige en vertrouwelijke informatie. Je neemt maatregelen om de vertrouwelijkheid te waarborgen. Op het portaal is actuele informatie over dit onderwerp te vinden. De ICT Servicedesk kan je helpen bij vragen over dit onderwerp.

3.2 Hoe te handelen bij een (vermeend) datalek

Als persoonsgegevens terecht zijn gekomen op een plek waar ze niet horen, meld je dit zo snel mogelijk bij de ICT Servicedesk of via het formulier "Melden datalek" op de pagina informatiebeveiliging & privacy (zie bijlage 1, Overige verwijzingen).

3.3 Bewaartermijnen

Het uitgangspunt is dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk. Wat noodzakelijk is hangt af van de situatie. Alle voorkomende bewaartermijnen staan beschreven in het document Archiefregeling (zie bijlage 1, Documenten).

3.4 Omgaan met intellectueel eigendom

Intellectueel eigendom is een verzamelnaam voor verschillende soorten rechten die creatieve werken beschermen. Gebruik van werk van anderen zonder toestemming is niet vanzelfsprekend. Voor bijvoorbeeld onderwijsdoeleinden, mogen sommige werken onder bepaalde voorwaarden worden gebruikt. Vraag je altijd af of en hoe het werk ingezet wordt en wat je hiervoor moet regelen. In de meeste gevallen geldt de grondslag "toestemming". In bijlage 1 staat een uitgebreidere toelichting over Auteurswet en auteursrecht in het onderwijs.

3.5 Online samenwerken: bestanden delen

Deel bij voorkeur bestanden via Teams of je OneDrive in plaats van deze te mailen. Door te delen heb je te allen tijde controle over de gegevens en kun je rechten intrekken of toekennen.

3.6 Online samenwerken: omgaan met e-mail

Bedenk voor je een e-mail stuurt of dit het meest efficiënte medium is en of je gevoelige informatie gaat versturen. Als je bestanden deelt, heeft het de voorkeur om deze te delen in plaats van als bijlage te versturen.

- Alle e-mail die vanuit het SintLucas-account wordt verzonden naar ontvangers buiten de organisatie, bevat een door SintLucas-vastgestelde disclaimer.
- Het cc-veld (carbon copy) gebruik je voor personen die je wilt informeren. Het bcc-veld (blind carbon copy) gebruik je als je de privacy wilt beschermen van ontvangers op het moment dat je meerdere mensen tegelijk een bericht of uitnodiging stuurt. Je voegt iemand daarmee toe aan de communicatie zonder dat anderen dit zien.
- Als je (grote) bestanden wilt delen met personen buiten de organisatie, verstuur je op een veilige manier met Zivver (zie bijlage 1, Overige verwijzingen). Zivver werkt zowel via Outlook als via <https://app.zivver.com>.
- SintLucas behoudt zich het recht voor bepaalde soorten inkomende en uitgaande e-mail of bijlagen te blokkeren of in quarantaine te plaatsen en na een bepaalde periode te verwijderen. Dit kan zowel via geautomatiseerde virusscanning als handmatig.
- Je persoonlijke e-mailadres is alleen voor gebruik op persoonlijke titel. E-mail mag niet anoniem of onder een fictieve naam verzonden worden, evenmin mag de naam van een ander worden gebruikt.
- Je kunt een niet persoonsgebonden e-mailadres aanvragen bij de ICT Servicedesk om met meerdere gebruikers te delen. Ieder gedeeld e-mailadres heeft een eigenaar die bekend is bij beheer en als aanspreekpunt is aangesteld.
- Wanneer de beveiliging of de continuïteit van de elektronische berichtenvoorziening dit vereist, is het College van Bestuur gerechtigd voor gebruikers bestemde berichten te laten lezen, kopiëren, te vernietigen of bijlagen te verwijderen.
- Het is niet toegestaan voor andere gebruikers bestemde e-mailberichten doelbewust ongeautoriseerd te lezen, kopiëren, wijzigen, door te sturen of te vernietigen.
- Vertrouwelijke en gevoelige informatie deel je met de grootst mogelijke zorgvuldigheid. Wanneer er geen andere mogelijkheid voorhanden is dan delen via e-mail, maak je gebruik van de mogelijkheid om berichten versleuteld te versturen via Zivver.

3.7 Online samenwerken: vergaderen

Gebruik voor online vergaderingen altijd MS Teams of Skype.

Als je jouw achtergrondomgeving op het beeld wilt afschermen, kun je je achtergrond vervangen of vervagen.

3.8 Omgaan met internet

Het internet biedt legio mogelijkheden om je werk goed uit te voeren, om te kunnen groeien in je werk en om trots en plezier over je functie of SintLucas als organisatie te laten zien. Ga hier verantwoordelijk mee om.

Het is niet toegestaan om:

- vertrouwelijke en gevoelige informatie op het internet te plaatsen, onbeveiligd via openbare netwerken te verspreiden, of op te slaan, tenzij met uitdrukkelijke toestemming van het management.
- software op het internet te plaatsen tenzij met uitdrukkelijke toestemming van de Manager Informatievoorziening.

- via internet/intranet (portaal) van diensten gebruik te maken, waarvoor een gebruiker niet is geautoriseerd.
- op het internet/intranet gebruik te maken van een naam van een ander.
- onethische informatie of informatie die strijdig is met de wet met behulp van ICT-faciliteiten van SintLucas te produceren, benaderen, op te slaan, te verzenden of in de openbaarheid te brengen. Onder deze informatie valt: pornografisch materiaal, informatie die de goede naam van SintLucas aantast, informatie die een discriminerend, opruiend, aanstootgevend of bedreigend karakter heeft.
- auteursrechtelijk beschermd materiaal, waaronder programmatuur, teksten, beeldmateriaal of muziek, te kopiëren, te downloaden of aan derden ter beschikking te stellen zonder toestemming van de auteursrechthebbende.

Bovendien moet bij het downloaden alles in het werk worden gesteld om het binnenhalen van virussen en andere kwaadaardige toepassingen te voorkomen en de beschikbaarheid van de ICT-faciliteiten niet in gevaar te brengen. Bij twijfels over de betrouwbaarheid van een bericht, neem je contact op met de ICT Servicedesk.

3.9 Gebruik van social media

SintLucas ondersteunt de open dialoog, de uitwisseling van ideeën en het delen van kennis van de gebruiker met vakgenoten en derden via sociale media. Richtlijnen over hoe om te gaan met social media vind je in het document "Social media protocol medewerkers" (zie bijlage 1, Documenten).

Deze punten zijn van belang met betrekking tot verantwoord digitaal werken:

- Het is niet toegestaan om foto-, film- en/of geluidsopnamen van school gerelateerde situaties, studenten, medewerkers of andere betrokkenen bij SintLucas (stagebedrijven, gastsprekers) op social media te zetten, tenzij de betrokkenen uitdrukkelijk toestemming voor plaatsing hebben gegeven.
- Het is niet toegestaan om vertrouwelijke (bijvoorbeeld persoonsgegevens) of gevoelige informatie (bijvoorbeeld financiële gegevens) over of van SintLucas op social media te plaatsen.

3.10 Ongewenst gebruik algemeen

Ongeacht welk medium je gebruikt om berichten te versturen, geldt: er mogen geen berichten verstuurd worden met een dreigende, seksueel intimiderende, racistische of op andere wijze aanstootgevende inhoud. Ook het verzenden van kettingbrieven, spam en/of reclameberichten, waarschuwingsberichten (hoax) van virussen aan (groepen) collega's is niet toegestaan.

4 Gebruik middelen en faciliteiten

4.1 Toegang ICT-faciliteiten

ICT-faciliteiten worden door het verantwoordelijk management ter beschikking gesteld aan jou als gebruiker. Onder ICT-faciliteiten verstaan we hardware zoals bijvoorbeeld laptops en telefoons maar ook software en licenties. Toegang tot middelen of het gebruik hiervan kan door het management beperkt worden tot onderdelen en/of diensten.

Als je vanuit je apparatuur gebruik maakt van de infrastructuur of ICT-faciliteiten van SintLucas, gelden hiervoor dezelfde regels als voor bedrijfsmiddelen die door SintLucas beschikbaar zijn gesteld. Je vindt deze regels in het Beleid bedrijfsmiddelen (zie bijlage 1, Documenten).

4.2 Gebruikersnaam en wachtwoord

- Elke gebruiker (met uitzondering van gastgebruikers) ontvangt een persoonlijke, op de op naam gebaseerde gebruikersnaam (inlogcode) voor de duur van zijn/haar contract of opdracht.
- Het wachtwoord is strikt persoonlijk, niet overdraagbaar en geheimhouding van het wachtwoord is verplicht. Als gebruiker neem je alle redelijke maatregelen voor de beveiliging en geheimhouding van dit wachtwoord.
- De gebruiker zal bij constatering van misbruik van zijn combinatie van gebruikersnaam en wachtwoord, zijn/haar leidinggevende/opdrachtgever hiervan onverwijld in kennis stellen en doet hiervan melding bij de ICT Servicedesk.
- Het wachtwoord kent een maximale houdbaarheid. De gebruiker ontvangt voor het verlopen van het wachtwoord een aantal e-mailnotificaties.
- Vergeten en verlopen wachtwoorden kunnen gewijzigd worden in het wachtwoordportaal: wachtwoord.sintlucas.nl.

4.3 Gebruik ICT-faciliteiten

SintLucas stelt alles in het werk er voor te zorgen dat de aangeboden apparatuur, software en licenties veilig zijn, zodat medewerkers op een veilige manier hun werk kunnen doen. Wij vragen je dan ook zoveel als mogelijk hiervan gebruik te maken en een melding in te dienen bij de ICT-Servicedesk als je iets mist om je werk goed te kunnen doen. Wij verwachten als SintLucas dat je op een professionele, verantwoorde, rechtmatige, ethische en redelijke en zorgvuldige wijze gebruik maakt van alle ICT-faciliteiten:

- Alle ICT-faciliteiten worden in beginsel gebruikt binnen het kader van de uit te voeren functie of opdracht bij SintLucas. Gebruik van deze faciliteiten voor persoonlijke doeleinden is toegestaan in eigen tijd (zoals de pauze), voor zover dit de dagelijkse werkzaamheden niet negatief beïnvloedt en niet schadelijk is voor de (prestaties van) ICT-faciliteiten van SintLucas en voor het netwerk, het gebruik beperkt is in tijdsduur en volgens de in dit document genoemde richtlijnen.
- Beperkte en tijdelijke opslag van privégegevens op de ICT-faciliteiten van SintLucas is toegestaan.
- Maak géén gebruik van USB-sticks of andere mobiel draagbare media, tenzij niet anders mogelijk is. Vertrouwelijke gegevens beveilig je door bijvoorbeeld de bitlockerfunctie aan te zetten (zie bijlage 1, Overige verwijzingen).
- Als gebruiker onderneem je geen acties of pogingen die de continuïteit of de beveiliging van ICT-faciliteiten van SintLucas ondermijnen.
- Print zo min mogelijk documenten. Draag zorg voor afgedrukte gegevens van vertrouwelijke aard en laat geen documenten onbeheerd achter in de printer of scanner.
- In geval van ziekte, onverwacht langdurige afwezigheid of nalatigheid van de gebruiker, is het College van Bestuur gerechtigd de leidinggevende toegang te geven tot specifieke bestanden of e-mails van de gebruiker. De Raad van Toezicht is gerechtigd toestemming te geven als het een lid van het College van Bestuur betreft.
Dit mag uitsluitend als kan worden aangetoond dat het onmogelijk is om toestemming van de gebruiker te krijgen en dit een zwaarwegende reden van bedrijfsbelang tot toegang oplevert. Privé-gemarkeerde bestanden of e-mails mogen niet bekeken worden, dit geldt ook voor e-mails die verzonden zijn dan wel afkomstig van een vertrouwenspersoon, bedrijfsarts, HR-adviseur en/of vakbond.
- De gebruiker laat mobiele apparatuur (laptop, smartphone, tablet etc.) nooit onbeheerd achter (ook niet in de kofferbak van je auto, in een leeromgeving, in een niet afgesloten ruimte).
- Bij verlies, diefstal of vermissing van mobiele apparatuur dient direct aangifte te worden gedaan bij de politie en melding te worden gemaakt bij de ICT Servicedesk. Na de aangifte lever je (een kopie van) het proces-verbaal zo snel als mogelijk in bij de ICT Servicedesk.

4.4 Veilig thuiswerken

Wees bij thuiswerken extra alert op berichten van onbekende afzenders. Neem in geval van twijfel altijd contact op met de ICT Servicedesk.

Andere aandachtspunten:

- Werk alleen in de door SintLucas vertrouwde omgevingen zoals Office365, Magister, Afas en OnStage.
- Werk bij voorkeur alleen op apparaten van SintLucas.
- Wees extra voorzichtig met persoonlijke gegevens, vooral op de privé-laptop en privé-telefoon.
- Verstuur bestanden met gevoelige informatie zoals persoonsgegevens alleen met Zivver.
- Wees alert op phishing berichten in de vorm van: e-mails, sms, apps of via telefoon. Klik niet zomaar op een link (zie bijlage 1, Overige verwijzingen).
- Let op welke apps je installeert. Installeer alleen betrouwbare apps.
- Controleer of een website veilig is. Wees extra alert op websites zonder slotje.
- Vergrendel ook thuis je computer als je iets anders gaat doen.

Meer informatie over dit onderwerp is te vinden op onze website bij Informatiebeveiliging & privacy (zie bijlage 1, Overige verwijzingen).

4.5 Omgaan met hardware en software

Het downloaden van illegale software en/of bestanden via het netwerk van SintLucas is ten strengste verboden. Dit geldt ook voor gebruik van teksten en afbeeldingen waarvoor auteursrechten verschuldigd zijn zonder toestemming van de auteur.

Je mag zelf software installeren op je apparaten. Voor software die niet namens of via SintLucas wordt aangeboden, geldt dat je hiervoor geen ondersteuning kunt vragen bij de ICT Servicedesk. Als gebruiker ben je volledig verantwoordelijk, en derhalve aansprakelijk, voor het nakomen van de voorwaarden die deze software stelt. Denk hierbij aan via internet geïnstalleerde (share-, free-) software. Whatsapp is een voorbeeld van niet door SintLucas ondersteunde software.

De op de desktop/laptop geregistreerde toepassingen zijn gebruikerseigendom van SintLucas. Alle bestanden die je opslaat in toepassingen van SintLucas vallen hieronder.

Het is niet toegestaan eigenmachtig wijzigingen aan te brengen in de hardware-configuratie van de desktop/laptop en andere draagbare apparatuur.

4.6 Opslaan van informatie

Je slaat alle informatie en bestanden op in de cloud of daarvoor bestemde applicaties van SintLucas. Het is niet toegestaan om informatie lokaal op te slaan, dus niet op het bureaublad en niet in de mappen op je apparaat. Dit geldt voor documenten, afbeeldingen, downloads, muziek en video's. Gebruik alleen USB-sticks of andere 'losse' informatiedragers als dit niet anders kan. Zorg dat je deze goed beveiligt.

Dynamische, niet-vastgestelde en gedeelde informatie voor een (beperkte) groep gebruikers voor een beperkte tijd wordt opgeslagen in een O365 groep of in Teams. Overige documenten sla je op in OneDrive.

Statische, formeel vastgestelde informatie wordt opgeslagen in deBieb (zie bijlage 1, Documenten).

5 Toezicht, controle, klachten en maatregelen

5.1 Recht op toezicht en controle

- SintLucas heeft het recht om met het oog op de naleving van deze richtlijn het gebruik van de ICT-faciliteiten te controleren en registreren. Controle vindt slechts plaats in het kader van deze richtlijn met in achtneming van de richtlijnen uit 5.2 Periodieke rapportages.
- Ten behoeve van controle op de naleving van de regels worden gegevens geautomatiseerd verzameld (gelogd). Deze gegevens zijn alleen toegankelijk voor de direct verantwoordelijke systeembeheerders en worden alleen in geanonimiseerde vorm aan overige beheerders en andere verantwoordelijken beschikbaar gesteld. Deze kunnen tot nadere technische maatregelen besluiten
- Bij vermoedens van overtreding van de regels kan controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.
- SintLucas houdt zich bij het controleren op het niveau van verkeersgegevens of persoonsgegevens onverkort aan de AVG en andere relevante wet- en regelgeving. In het bijzonder beveiligt de SintLucas de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang daartoe contractueel verplicht tot geheimhouding.

5.2 Periodieke rapportages

- Periodiek wordt gerapporteerd over het gebruik van de ICT-faciliteiten. Hierbij kunnen onder meer de tijdsbesteding en de verkeersgegevens van bezochte sites, verstuurd e-mail en gebelde telefoonnummers op algemeen niveau worden vastgelegd en beoordeeld.
- In het geval dat de periodieke rapportages aanleiding geven tot het vermoeden van ontoelaatbaar gebruik van de ICT-faciliteiten, dat wil zeggen gebruik dat in strijd is met de belangen die met de in de inleiding genoemde doeleinden beoogd worden en de verdere inhoud van deze richtlijn, kan SintLucas het gebruik van deze middelen op individueel niveau controleren.
Het gebruik van deze middelen kan eveneens op individueel niveau gecontroleerd worden indien op andere wijze een redelijke verdenking of een vermoeden van ontoelaatbaar gebruik bestaat. Vooraf aan de controle wordt aan het College van Bestuur toestemming gevraagd en wordt de FG-er geïnformeerd. Indien het ontoelaatbaar gebruik door de FG-er gepleegd, dan wordt zijn/haar leidinggevende vooraf om toestemming gevraagd. Wanneer het een lid van het College van Bestuur betreft, wordt toestemming verleend door de Raad van Toezicht. Meer informatie hierover is te vinden in het IBP-beleid (zie bijlage 1, Documenten).

- Deze controle zal slechts door enkele daartoe geautoriseerde personen kunnen worden uitgevoerd. De autorisatie voor deze controle kan uitsluitend verleend worden door het College van Bestuur. Met betrekking tot de positie en integriteit van deze personen en de controle daarop heeft SintLucas de nodige voorzieningen getroffen.
- Een controle op individueel niveau zal plaatsvinden indien het beoogde doel de controle rechtvaardigt. Het controlemiddel dat het minst inbreuk maakt op de privacy van de betreffende gebruiker zal het eerst worden toegepast. Naarmate de verdenking toeneemt op grond van de uit de analyse verkregen gegevens, kan een zwaarder controlemiddel worden toegepast.
- Bij ernstig vermoeden van of geconstateerde (beveiliging)incidenten heeft de manager Informatievoorziening het recht om apparatuur en/of gebruikers de toegang tot computers en/of netwerken (tijdelijk) te ontfemen.
- Indien hiertoe gedwongen of gesommeerd door een vertegenwoordiging van de rechterlijke macht, zal het College van Bestuur medewerking verlenen aan verstrekking van informatie aangaande gebruik van ICT-faciliteiten door individuele gebruikers.

5.3 Klachten

In het geval dat een gebruiker zich over de niet-nakoming van deze richtlijn door SintLucas wenst te beklagen, dan kan de gebruiker informatie over de klachtenregeling vinden in de Klachtenregeling Stichting SintLucas (zie bijlage 1, Documenten).

Wanneer het specifieke klachten betreft over de (naleving) van de AVG, kunnen deze rechtstreeks worden gemeld bij de Functionaris voor Gegevensbescherming via privacy@sintlucas.nl.

5.4 Rechtspositionele maatregelen

SintLucas behoudt zich het recht voor afhankelijk van de overtreding, frequentie en de omstandigheden van het geval rechtspositionele maatregelen te nemen, waaronder ontslag op staande voet, ontbinding en opzegging van de (arbeids)overeenkomst.

In geval van overtreding van de in deze richtlijn opgenomen regels en voorwaarden gelden de volgende bepalingen:

- Bij constatering van misbruik van ICT-faciliteiten of het gebruik in strijd met de regelgeving of wettelijke bepalingen, kan het College van Bestuur een sanctie opleggen conform wat hierover met betrekking tot op non actief stelling, disciplinaire straffen, beëindiging van het dienstverband en ontslag is vastgelegd in de CAO en wet- en regelgeving.

6 Overige bepalingen

Deze richtlijn is gepubliceerd op het portaal. In geval van vragen neem je contact op met de manager Informatievoorziening of ICT Servicedesk.

Voor het gebruik van deze richtlijn verantwoord digitaal werken gelden binnen SintLucas de volgende bepalingen:

- Vaststelling van deze richtlijn geschiedt door het College van Bestuur volgens de gangbare besluitvormingsprocedure.
- Het College van Bestuur informeert de gebruikers voorafgaande aan de invoering en bij wijziging van deze richtlijn over de inhoud van deze code waaronder wat over toezicht en controle is opgenomen.
- Evaluatie van de inhoud en de werking van deze richtlijn vindt jaarlijks plaats en/of in geval van ingrijpende wijzigingen binnen de organisatie en/of het gebruik van ICT-faciliteiten.
- In gevallen waarin deze richtlijn niet voorziet, beslist het College van Bestuur.

7 Bijlage 1 Verwijzingen en links

7.1 Documenten

Alle in deze richtlijn genoemde beleidsstukken zijn vastgesteld en staan in [DeBieb](#):

- Informatiebeveiligings- en privacybeleid (IBP-beleid)
- Archiefregeling
- Social media protocol medewerkers
- Beleid bedrijfsmiddelen
- Klachtenregeling SintLucas

7.2 Overige verwijzingen:

- [Melden datalek](#)
- [Informatie over Zivver](#)
- Bitlockerfunctie
- [Informatie over Phishing](#)
- Informatie over veilig (thuis)werken wordt regelmatig bijgewerkt. Je vindt deze op de pagina [Informatiebeveiliging en privacy](#) en je kunt je aanmelden voor deze groep in [Yammer](#).

7.3 Toelichting Auteurswet en auteursrecht in het onderwijs

Als auteursrechtelijk beschermd werk gebruikt wordt voor onderwijsdoeleinden, vallend in het leerplan (het curriculum) en zonder winstoogmerk, dan mag dit onder bepaalde voorwaarden worden gebruikt. Het werk mag niet dienen als versiering van onder andere lesbrieven. Voor dat gebruik is expliciete toestemming nodig. Het gaat hier om onderwijs dat uit naam van de overheid of door een rechtspersoon zonder winstoogmerk wordt gegeven. Zo mag bijvoorbeeld een afbeelding van een kunstwerk worden getoond om dat te bespreken als dat in het leerplan staat, maar mag datzelfde kunstwerk niet als versiering in het lokaal hangen. Als binnen het werk sprake is van een portret zullen ook de richtlijnen van de AVG gevolgd moeten worden. In de meeste gevallen geldt dan de grondslag 'Toestemming'.

Wat de bron is van het originele werk maakt niet uit. Werken die op internet staan kunnen onder de "onderwijsexceptie" vallen maar dat is niet vanzelfsprekend. Ook dient altijd rekening te worden gehouden met de persoonlijkheidsrechten van de maker(s). Je mag het werk niet aantasten en de maker heeft het recht op zijn naamsvermelding bij het werk. Voor al het overige gebruik van auteursrechtelijk beschermd werk, bijvoorbeeld tijdens de diploma-uitreiking of een feestavond, is toestemming wél nodig en moet er ook een vergoeding worden betaald. Ondanks toegestaan gebruik zonder toestemming kan ook dan een billijke vergoeding zijn verschuldigd. Daar zijn collectieve regelingen voor getroffen (o.a. Buma/Stemra, Reprorecht, Videma).

Voor de docent is het dus verstandig zich af te vragen hoe werk wordt ingezet/gebruikt. Gebruik zonder toestemming is niet vanzelfsprekend.

Toestemming vragen, bijvoorbeeld via e-mail, aan de rechthebbende van werk is in veel gevallen daarom aan te bevelen.