# Reglement gebruik ICT-faciliteiten Summa

(2024)

**Colofon**

*Bij de totstandkoming van dit reglement is gebruik gemaakt van informatie uit het document 'Verantwoord netwerkgebruik' (IBPDOC26) uit het Framework IBP van saMBO-ICT/Kennisnet.*

SUMMA

# Inhoudsopgave

# 1 Inleiding

Summa stelt ICT-faciliteiten ter beschikking aan medewerkers, studenten en gasten. Dat varieert van gebruik van het wifi-netwerk en internet tot het ter beschikking stellen van apparaten en software/toepassingen. Het gebruik hiervan is voor medewerkers essentieel om hun werk te kunnen doen en voor studenten om hun studie te volgen. Aan het gebruik van deze faciliteiten kunnen echter ook risico's verbonden zijn voor Summa. Tegen de achtergrond van deze risico's mag van de gebruiker verantwoord gebruik van ICT-faciliteiten worden verwacht en mag Summa eisen stellen ten aanzien van het gebruik.

Met dit reglement stelt Summa regels omtrent het aanvaardbaar en gewenst gebruik van ICT-faciliteiten. Daarbij is gestreefd naar een balans tussen verantwoord en veilig gebruik van ICT-faciliteiten en de privacy van de gebruiker.

Het gebruik van sociale media is niet weg te denken, maar brengt ook risico's met zich mee. Daarom zijn in dit reglement ook gedragsregels met betrekking tot het gebruik van sociale media opgenomen.

# 2 Algemene bepalingen

## 2.1 Belangrijke begrippen

In dit reglement worden verschillende begrippen gebruikt. Die hebben voor dit reglement de volgende betekenis.

*Beheerder:* Een medewerker die in het kader van zijn functie beheerswerk-zaamheden verricht en daarom beschikt over verregaande bevoegdheden binnen ICT-faciliteiten.

*Dienst IT:* De dienst die binnen Summa is belast met het inrichten, onderhouden en beveiligen van de ICT-faciliteiten.

*Gebruiker:* Iedereen die gebruik maakt van de ICT-faciliteiten die door Summa ter beschikking worden gesteld. Hierbinnen kan onderscheid worden gemaakt tussen:

a. *Medewerker*: persoon die werkt voor en/of in opdracht van Summa. Dat kan zijn op basis van een arbeidsovereenkomst met Summa, maar ook op basis van inhuur, detachering of dienstverleningsovereenkomst.

b. *Student*: persoon die is ingeschreven als student of leerling bij een van de opleidingen van Summa.

c. *Gast*: persoon die geen medewerker of student is, maar wel rechtmatig toegang heeft tot ICT-faciliteiten van Summa.

*ICT-faciliteiten:* De door of namens Summa aan gebruikers ter beschikking gestelde faciliteiten, zoals bijvoorbeeld netwerkfaciliteiten, internet, hardware (pc's, laptops, tablets, telefoons, printers, etc.), software (e-mail, applicaties, cloudservices, besturingssystemen, etc.) en andere digitale hulpmiddelen (robots, etc),

*Sociale media:* De verzamelnaam voor online platforms waar (voornamelijk) gebruikers zorgen voor inhoud. Bijvoorbeeld door in beeld, geluid of tekst met anderen te communiceren of informatie te delen.

## 2.2 Uitgangspunten

1. Summa stelt ICT-faciliteiten beschikbaar aan de gebruiker voor werk of het volgen van een opleiding. Het gebruik van de ICT-faciliteiten is verbonden aan deze doelen en moet daarmee verenigbaar zijn.
2. Dit reglement heeft als doel het gebruik van ICT-faciliteiten in goede banen te leiden en doet dit door regels te stellen ten aanzien van:
   - beveiliging;
   - bescherming van persoonsgegevens[1];
   - bescherming van (vertrouwelijke) informatie van Summa;

[1] Persoonsgegevens zijn alle gegevens die iets zeggen over een bepaalde persoon. Voorbeelden zijn: naam en achternaam; adres; locatiegegevens op een mobiele telefoon; IP-adres; gezondheidsgegevens; studievoortgang, enz.

- sociale veiligheid;
- bescherming van intellectuele eigendomsrechten en licentie-afspraken;
- gebruik van de ICT-faciliteiten;
- gebruik van sociale media; en
- toezicht op gebruik van ICT-faciliteiten en naleving van dit reglement.

3. Dit reglement is niet uitputtend bedoeld. Dat iets niet is opgenomen in dit reglement betekent niet dat er geen eisen zijn of het gebruik vrij is, maar dat het gebruik moet voldoen aan de bepalingen uit dit reglement, voor zover die redelijkerwijs kunnen worden toegepast op de niet-beschreven situatie.
4. Het reglement geldt voor alle gebruikers van ICT-faciliteiten van Summa.
5. Dit reglement is plaats en tijd onafhankelijk. Daarmee is het ook van toepassing buiten de locaties van Summa of als met eigen apparaten gebruik wordt gemaakt van ICT-faciliteiten. Bijvoorbeeld: bij thuiswerken of als vanuit het buitenland via internet op afstand wordt ingelogd.

## 2.3 Verantwoordelijkheid gebruiker

1. Gebruikers zijn te allen tijde aanspreekbaar op het naleven van het bepaalde in dit reglement.
2. Bij een vermoeden van misbruik moet een gebruiker zijn wachtwoord direct wijzigen en melding maken van het (mogelijke) misbruik bij het Servicepunt. (door een melding te maken op de Selfserviceportal, door te mailen naar servicepunt@summacollege.nl of door bellen naar 040 269 4411.) ;
3. Het gebruik van ICT-faciliteiten is persoonlijk en de verantwoordelijkheid van de gebruiker, ook als met eigen apparaten gebruik wordt gemaakt van de ICT-faciliteiten. Dat betekent bijvoorbeeld dat persoonlijke inlogcodes niet met anderen worden gedeeld, dat de gebruiker sterke wachtwoorden gebruikt, dat Summa-eigendommen niet met anderen worden gedeeld en dat bij het toegang geven tot eigen apparaten waarop Summa-werkzaamheden worden uitgevoerd de gebruiker ervoor zorgt dat dit op een veilige manier gebeurt.
4. Het gebruik van de ICT-faciliteiten is voor gebruikers nodig om werk of leren te ondersteunen en het is niet toegestaan de ICT-faciliteiten voor andere doeleinden te gebruiken. Beperkt privégebruik van ICT-faciliteiten is toegestaan, mits het werken en/of leren er niet onder lijden, het niet storend is voor anderen en het geen storende invloed heeft op de goede werking of beschikbaarheid van ICT-faciliteiten.
5. Het gebruik van eigen apparatuur en/of toepassingen op de ICT-faciliteiten van Summa is toegestaan onder voorwaarde dat dit gebruik voldoet aan de regels van dit reglement en eventuele door Summa te stellen eisen. Summa kan de eisen en/of voorwaarden te allen tijde wijzigen.

## 2.4 Handhaving

1. Bij een overtreding van het bepaalde in dit reglement of een vermoeden van misbruik van een wachtwoord of beveiligingsmaatregel kan het betreffende account door een beheerder per direct ontoegankelijk worden gemaakt.
2. Summa zal bij overtredingen handhavend optreden, (disciplinaire) maatregelen kunnen worden opgelegd indien daar aanleiding toe is.

## 2.5 Noodsituaties

1. Bij calamiteiten en andere onvoorziene situaties die naar het exclusieve oordeel van Summa een bedreiging vormen voor de continuïteit van het onderwijs en/of de bedrijfsvoering kan Summa maatregelen nemen die afwijken van het bepaalde in dit reglement en die het gebruik van ICT-faciliteiten (tijdelijk) geheel of gedeeltelijk beperken.
2. Summa is niet aansprakelijk voor de gevolgen van het geheel of gedeeltelijk beperken van (de toegang tot) ICT-faciliteiten.

# 3 Algemeen

## 3.1 Algemene normen

1. Gebruikers moeten zich (laten) informeren over passende beveiligingsmaatregelen. Gebruikers hanteren de door Summa ingestelde en toegepaste beveiligingsmaatregelen. Het omzeilen of beperken ervan is niet toegestaan.
2. Wachtwoorden en pincodes zijn persoonlijk en worden niet gedeeld. Ook worden ze niet opgeschreven en bij het apparaat of de toepassing bewaard. Gebruikers houden bij het samenstellen van wachtwoorden en pincodes rekening met het wachtwoordbeleid en zorgen ervoor dat ze verschillende en sterke wachtwoorden en pincodes gebruiken voor verschillende systemen, toepassingen, enzovoorts. Summa kan voorschriften opstellen voor wachtwoorden, pincodes en verificatiecodes (wachtwoordbeleid)
3. Gebruikers mogen de ICT-faciliteiten niet gebruiken voor activiteiten waarvan redelijkerwijs kan worden begrepen dat deze illegaal of verboden zijn en/of de naam en reputatie van Summa kan schaden.

## 3.2 Toegang

1. Iedere gebruiker krijgt voor eigen gebruik een gebruikersaccount met een persoonlijke inlognaam en wachtwoord. De gebruiker gaat zorgvuldig om met deze gegevens: de persoonlijke inlognaam mag alleen functioneel worden gedeeld en het wachtwoord mag met niemand worden gedeeld.
2. Zodra een gebruiker inlogt op het netwerk worden de activiteiten van de gebruiker vastgelegd (logging). Indien daar aanleiding toe is kan via deze logging het gebruik van het netwerk, faciliteiten, toepassingen, enzovoorts, worden achterhaald. Gebruiker mag deze logging niet beperken, verhinderen, aanpassen, verwijderen of anderszins manipuleren; iedere poging hiertoe wordt gezien als misbruik en is aanleiding tot maatregelen.

## 3.3 Vertrouwelijkheid

1. Indien een gebruiker (onbedoeld) toegang krijgt tot vertrouwelijke informatie of privacygevoelige informatie, bijvoorbeeld persoonsgegevens, behandelt hij deze informatie strikt vertrouwelijk.
2. Door Summa opgestelde voorschriften die de vertrouwelijkheid van informatie, persoonsgegevens en intellectuele eigendomsrechten waarborgen moeten door de gebruiker worden opgevolgd.
3. Summa heeft en houdt zeggenschap over de informatie van Summa, een gebruiker heeft geen zeggenschap over deze informatie, tenzij deze vooraf expliciet is toegekend door Summa.

## 3.4 Classificatie vertrouwelijkheid gegevens

1. Summa maakt bij de beoordeling van vertrouwelijkheid van gegevens gebruik van de volgende indeling en classificatie:
    a. Openbare gegevens; dit zijn gegevens die juist voor publicatie bedoeld zijn, ze zijn niet vertrouwelijk of geheim;

b. Interne gegevens; dit zijn gegevens die alleen voor gebruik en verwerking binnen Summa bedoeld zijn. Het gaat bijvoorbeeld om financiële gegevens, afspraken met studenten, leveranciers of medewerkers, inkoopprijzen, licentieprijzen, et cetera. Deze gegevens worden niet publiek gedeeld via e-mail, website of intranet. Deze informatie wordt slechts met derden gedeeld indien dit noodzakelijk is en de uitwisseling van deze informatie veilig kan plaatsvinden;
c. Vertrouwelijke gegevens; dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers of studenten binnen Summa toegankelijk zijn. Het gaat in ieder geval om persoonsgegevens, vertrouwelijke afspraken, afspraken rondom veiligheid en integriteit, studentgegevens waaronder (afspraken rondom) zorg, begeleiding en gezondheid, of personeelsgegevens. Deze gegevens worden alleen verzameld, gebruikt en gedeeld als dit noodzakelijk is en het gebruik van deze gegevens is toegestaan in een wet, regelgeving, afspraak of als de persoon waarop deze gegevens betrekking hebben hier toestemming voor heeft gegeven. Uitwisselen van deze informatie moet veilig geschieden en (toegang tot) deze informatie wordt met een toegangscode, wachtwoord of pincode beveiligd. In het register van verwerkingen wordt bijgehouden welke persoonsgegevens tussen systemen uitgewisseld worden en op basis van welke grondslag dit gebeurt.

## 3.5 Melden datalek of beveiligingsincident

1. In geval een gebruiker interne of vertrouwelijke informatie heeft gedeeld of denkt te hebben gedeeld met een persoon of organisatie die deze informatie niet mocht ontvangen, zal de gebruiker dit zo snel mogelijk melden bij het Servicepunt. De gebruiker houdt zich beschikbaar voor het opvolgen van instructies van de Dienst IT om mogelijke nadelige gevolgen te voorkomen of (verder) te beperken.
2. Indien een gebruiker weet heeft van of een vermoeden heeft van een beveiligingsincident of datalek dan wordt hiervan melding gedaan bij het Servicepunt.
3. Een gebruiker die bekend is of wordt met een zwakke plek in één van de systemen, software of applicaties van Summa, meldt dit bij het Servicepunt. Summa volgt hierbij het beleid ‘responsible disclosure’ (https://www.summacollege.nl/juridisch/responsible-disclosure).
4. Het Servicepunt is te bereiken door een melding te maken op de Selfserviceportal voor medewerkers, of door te mailen naar servicepunt@summacollege.nl. In dringende gevallen kan op werkdagen (van 8.00 – 16.30 uur) contact op worden genomen via 040 269 4411. Kijk voor meer contactinfo: Servicepunt Contact & feedback - SelfServicePortal (topdesk.net) voor de

# 4 Medewerkers

## 4.1 Vertrouwelijkheid

1. Medewerkers gaan zorgvuldig om met persoonsgegevens, Summa-specifieke en vertrouwelijke informatie. Dat betekent onder andere dat deze gegevens en informatie alleen op de daarvoor aangewezen en door Summa beheerde systemen worden opgeslagen. Het is niet toegestaan deze op te slaan op persoonlijke systemen of in persoonlijke cloud-toepassingen. Het betekent ook dat medewerkers voorkomen dat deze gegevens en informatie zichtbaar zijn/is voor onbevoegden en dat deze niet mee kunnen kijken (clear screen, clear desk, aansluiten van extra beeldschermen, etc.).
2. Persoonsgegevens, Summa-specifieke en vertrouwelijke informatie worden bij voorkeur niet via e-mail verstuurd (ook niet als bijlage), maar vanuit Teams, SharePoint en OneDrive of via SURFfilesender. Mocht het niet anders kunnen, dan wordt gekozen voor encryptie en/of wachtwoordbeveiliging.
3. Het gebruik van mobiele gegevensdragers, zoals bijvoorbeeld usb-sticks, geheugenkaarten of discs, wordt waar mogelijk vermeden. Medewerkers die ervoor kiezen een mobiele gegevensdrager in te zetten zorgen daarbij voor passende beveiliging/versleuteling, zoals bijvoorbeeld het via het Summa-netwerk beschikbare Bitlocker.
4. Diefstal of verlies van informatie, persoonsgegevens of apparaten wordt na constatering zo snel mogelijk gemeld via het Servicepunt of Topdesk (Selfserviceportal).
5. Interne gegevens, vertrouwelijke informatie en persoonsgegevens van, verwerkt door of in beheer bij Summa, mogen niet voor eigen persoonlijke doeleinden worden gebruikt.

## 4.2 Summa-apparaten (desktops, laptops, tablets, etc.)

1. Summa stelt apparatuur en toepassingen beschikbaar met een standaard-configuratie. De medewerker mag eenvoudige aanpassingen doen (bijvoorbeeld lettertype, soort webbrowser) en toepassingen installeren, maar aanpassingen die gevolgen kunnen hebben voor de beveiliging of andere gebruikers mogen alleen worden gedaan na toestemming van een beheerder. Het is de verantwoordelijkheid van de medewerker dat hij zich vooraf door een beheerder laat informeren over de mogelijke gevolgen van een aanpassing of installatie.
2. Het is de medewerker niet toegestaan om technische aanpassingen te doen aan Summa-apparaten.
3. Bij het tijdelijk verlaten van zijn werkplek en of het onbeheerd achterlaten van het apparaat dient de medewerker het apparaat altijd te vergrendelen (Windowstoets + l). Bij het verlaten van de werkplek en/of aan het einde van de werkdag/werkzaamheden moet worden uitgelogd en/of afgesloten; informatie op papier wordt opgeborgen (clear desk).
4. Laat de medewerker een werkdevice aan het einde van de werkdag bij Summa achter, dan dient deze uit het zicht te worden opgeborgen in een afgesloten ruimte (in bureaulade of kast; niet op een tafel in een werkkamer).
5. Zodra er een melding is van een update wordt deze zo snel mogelijk (uiterlijk binnen 1 werkdag) uitgevoerd.
6. De Dienst IT voert op de Summa-apparaten - op afstand- (preventief) onderhoud uit en verhelpt storingen. De medewerker verleent hieraan zijn medewerking. De medewerker is ervan op de hoogte dat hierbij mogelijk toegang nodig is tot de persoonlijke digitale werkomgeving van de medewerker.

## 4.3 Bring your own device (BYOD)

1. Het is medewerkers toegestaan om eigen apparatuur te gebruiken voor de Summa-werkzaamheden. Het beheer en het toepassen van adequate beveiligingsmaatregelen (denk bijvoorbeeld aan toegankelijkheid, maatregelen tegen virussen en malware, het zo snel mogelijk uitvoeren van updates en versleuteling) zijn dan de verantwoordelijkheid van de medewerker. Het bepaalde in dit reglement geldt ook bij BYOD.
2. Bij het tijdelijk verlaten van zijn werkplek en of het onbeheerd achterlaten van het eigen apparaat dient de medewerker het apparaat te vergrendelen.
3. Het aansluiten van eigen netwerkapparatuur (zowel bedraad, als draadloos) waarmee de verbinding kan worden gedeeld met derden is verboden.
4. Summa stelt software en toepassingen ter beschikking. Deze mogen op het eigen apparaat worden geïnstalleerd en gebruikt voor het uitoefenen van de Summa-werkzaamheden.
5. Indien een medewerker een eigen apparaat niet langer gebruikt voor zijn Summa-werkzaamheden of Summa verlaat verwijdert hij definitief
   - geïnstalleerde software en toepassingen, en
   - eventueel aanwezige gegevens van Summa.
6. Summa mag een medewerker vragen aan te tonen dat het eigen apparaat voldoet aan alle maatregelen. Summa kan een medewerker die dit niet kan aantonen verbieden een eigen apparaat te gebruiken.
7. Blj het gebruik van eigen apparatuur in het kader van de werkzaamheden ten behoeve van Summa kan het gebruik van software en applicatie(s) van Summa worden vastgelegd (gelogd) in het kader van informatiebeveiliging en integriteit van de gegevens en netwerk van Summa. In dat kader kan informatie (bestanden, cookies) op deze eigen apparatuur worden geplaatst.

## 4.4 Software, digitaal lesmateriaal en intellectueel eigendom

1. Software en/of digitaal lesmateriaal mogen alleen worden geïnstalleerd/gebruikt met de juiste licenties.
2. Software en/of digitaal lesmateriaal mogen alleen worden geïnstalleerd/gebruikt nadat de medewerker heeft gecontroleerd of het veilig kan worden gebruikt.
3. Onder veilig gebruik wordt ook verstaan het mogelijk verwerken van persoonsgegevens. Indien er persoonsgegevens worden verwerkt in opdracht van Summa moet voorafgaand aan het gebruik van de software en/of het digitaal lesmateriaal een overeenkomst en een verwerkersovereenkomst worden gesloten.
4. Medewerkers respecteren de intellectuele eigendomsrechten van Summa en/of derden en de binnen Summa geldende licentieafspraken.

## 4.5 Toegang tot de persoonlijke werkomgeving medewerker

1. In geval van ongeplande, onverwachte of onverwacht-langdurige afwezigheid van een medewerker, waarbij de medewerker niet heeft (kunnen) voorzien in vervanging tijdens afwezigheid en het niet mogelijk is toestemming te vragen aan de medewerker, heeft de directeur IT van de Dienst IT de mogelijkheid om toegang te verschaffen tot de persoonlijke werkomgeving van de medewerker indien:
   a. de Functionaris voor Gegevensbescherming, geraadpleegd door de directeur IT, hierover een positief advies heeft uitgebracht, en

   b. dit strikt noodzakelijk is voor de voortgang van de taken en werkzaamheden van Summa en
   c. de terugkeer van de medewerker (langer) kan worden afgewacht.
2. Inzage of toegang wordt slechts verleend in aanwezigheid van tenminste twee personen die samen hun werkzaamheden vastleggen in een verslag. De medewerker wordt hierover geïnformeerd en krijgt een afschrift van dit verslag.

# 5 Studenten en gasten

## 5.1 Vertrouwelijkheid

1. Studenten krijgen tijdens hun opleiding gegevens van andere personen, bijvoorbeeld contactgegevens van andere studenten. Studenten die persoonsgegevens ontvangen zullen hier zorgvuldig mee omgaan en deze niet gebruiken voor andere doelen dan waarvoor ze zijn gegeven.
2. Studenten die hun laptop tijdelijk onbeheerd achterlaten, vergrendelen het apparaat altijd (Windowstoets + l). Zodoende kunnen anderen geen onbedoelde toegang krijgen tot de laptop en via deze laptop tot de ICT-faciliteiten van Summa.

## 5.2 Apparatuur

1. Een student die gebruik maakt van Summa-computers, -voorzieningen en/of randapparatuur zal dat zorgvuldig en verantwoord doen, zodat ook anderen (later) nog hiervan gebruik kunnen maken.
2. Summa-computers en –voorzieningen zijn terug te leiden naar Summa: studenten zullen hiermee geen activiteiten ondernemen die strijdig zijn met wet- en regelgeving, de naam en reputatie van Summa kunnen beschadigen of derden op welke manier dan ook kunnen benadelen.

## 5.3 Gasten

1. Gasten kunnen met een gastaccount beperkte toegang krijgen tot de ICT-faciliteiten van Summa, bijvoorbeeld wifi-toegang.
2. Gasten mogen hiermee geen activiteiten ondernemen die strijdig zijn met wet- en regelgeving, de naam en reputatie van Summa kunnen beschadigen of derden op welke manier dan ook kunnen benadelen.

# 6 Online communicatie, internet en *social media*

## 6.1 Online communicatie algemeen

1. Bij communicatie via digitale kanalen wordt normaal taalgebruik gebruikt en het moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie.
2. Communicatie via digitale kanalen mag niet
   - dreigend,
   - beledigend,
   - seksueel getint,
   - racistisch,
   - discriminerend of
   - anderszins aanstootgevend zijn.
3. Gebruikers delen geen informatie die vertrouwelijk is of privacygevoelige informatie over medewerkers en studenten.
4. Gebruikers die geen formele woordvoerder van Summa zijn moeten zich realiseren dat zij alleen een persoonlijk standpunt kunnen uiten; bij uitingen dienen zij hier rekening mee te houden en aan te geven dat een uiting een persoonlijke uiting is en niet een formeel standpunt van Summa.
5. Medewerkers zijn het gezicht van de organisatie. Dit geldt vooral voor bestuurders, leidinggevenden en zij die werken in het primaire proces. Zij dienen zich bewust te zijn van het feit dat de grens tussen werk en privé niet scherp is. Hierdoor kunnen foto's en uitingen die privé zijn geplaatst zakelijk doorwerken. Voorkom dat privéuitingen op social media de belangen van Summa schaden. Respecteer algemene omgangsvormen; plaats nooit bedreigende of racistische berichten. Dit geldt voor zowel voor platformen waar je je profileert als Summa-medewerker (bijv. LinkedIn) als voor bijv. Facebook waar je jezelf als privépersoon uit.
6. Iedere gebruiker is zelf verantwoordelijk voor wat er in zijn naam wordt gecommuniceerd.

## 6.2 Internet

1. Het gebruik van internet moet in relatie staan tot werk of opleiding; beperkt privégebruik is toegestaan.
2. Niet toegestaan is:
   a. het bezoeken van aanstootgevende websites,
   b. het verspreiden van aanstootgevend materiaal,
   (met *aanstootgevend wordt bijvoorbeeld bedoeld: pornografisch, racistisch, discriminerend, beledigend, (seksueel) intimiderend of aanzettend tot haat en geweld),*
   c. het onbevoegd toegang krijgen tot of belemmeren van systemen en gegevens die via internet te benaderen zijn,
   d. het downloaden van materialen die auteursrechtelijk zijn beschermd of die alleen met een geldige licentie mogen worden gebruikt,
   e. commercieel gebruik of andere vormen van geldelijk of persoonlijk gewin.

## 6.3 Social media

1. Gebruikers moeten zich bewust zijn van de impact van social media en daarom rekening houden met goede naam en reputatie van Summa en iedereen die hier werkt, leert of op een andere manier betrokken is bij Summa.
2. De verboden uit artikel 6.1, tweede lid, en 6.2, tweede lid, gelden ook voor het gebruik van social media.
3. Gebruikers plaatsen geen beeldmateriaal, gemaakt in relatie tot activiteiten van Summa, zonder voorafgaande duidelijke toestemming van de personen die hierop zijn afgebeeld.

## 6.4 Opnames en beeldmateriaal maken en gebruiken

1. Gebruikers mogen geen foto's, beeld- of geluidsopnames maken op Summa-locaties of tijdens Summa-activiteiten zonder voorafgaande toestemming van een docent of leidinggevende. Zijn er personen duidelijk herkenbaar aanwezig, dan is ook van deze personen voorafgaande toestemming nodig.
2. Toestemming tot het maken van een opname betekent geen (automatische) toestemming voor publicatie, in welke vorm dan ook, tenzij dit nadrukkelijk is gevraagd vóór het maken van de opname. Eventueel moet deze toestemming alsnog en vóór publicatie worden gevraagd aan betrokkenen.

# 7 Handhaving

## 7.1 Onderzoek

1. Om cyberaanvallen te voorkomen, dan wel tijdig te onderkennen en om misbruik van accounts en informatie van Summa te voorkomen wordt 24/7 gecontroleerd op verdachte netwerkactiviteiten en misbruik van ICT faciliteiten. Hiertoe wordt gebruik gemaakt van monitoring en logging (logbestanden).
2. Indien uit de monitoring blijkt van (een vermoeden van) misbruik door derden van een account of ICT-faciliteit, kan een Beheerder van de Dienst IT om (verdere) nadelige gevolgen te voorkomen of beperken, hierover contact opnemen met de gebruiker via de bij Summa bekende contactgegevens van de gebruiker. Tevens kan de toegang tot de ICT faciliteiten tijdelijk worden beperkt totdat de gebruiker contact heeft gehad met de Dienst IT hierover.
3. Bij een vermoeden van overtreding van de bepalingen uit dit reglement kan hiervan melding worden gedaan:
   - voor studenten bij de teamleider van de opleiding,
   - voor medewerkers bij de leidinggevende.
   Afhankelijk van de aard van de melding en/of de overtreding zal dan worden bepaald hoe een en ander wordt onderzocht.
4. De directeur IT, hiertoe gemandateerd door het CvB, kan bij een vermoeden van misbruik en/of overtreding, na advies ingewonnen te hebben de Functionaris voor Gegevensbescherming een onderzoek instellen. Dat kan op eigen initiatief of op verzoek van een belanghebbende. Bij dat onderzoek kan toegang worden verkregen tot de persoonlijke omgeving en/of bestanden van de gebruiker . Onderzoek wordt gedaan door twee personen die samen een verslag opstellen van het onderzoek.
5. Een onderzoek hoeft niet vooraf te worden gemeld aan de gebruiker, maar achteraf wordt de gebruiker geïnformeerd over het onderzoek en de uitkomst.
6. De onderzoeksresultaten en het verslag worden niet langer bewaard dan nodig en vernietigd zodra duidelijk is dat bewaring hiervan niet (langer) nodig is.

## 7.2 Maatregelen

1. Als een gebruiker de bepalingen uit dit reglement niet naleeft kunnen maatregelen worden getroffen. Deze zijn afhankelijk zijn van de ernst van de overtreding en kunnen variëren. Het gebruik van ICT-faciliteiten kan worden ontzegd door de directeur IT. Een medewerker kunnen disciplinaire maatregelen worden opgelegd, zoals bedoeld in de cao mbo, voor een student geldt dat het kan leiden tot verwijdering.
2. Als er door het niet-naleven van de bepalingen schade is ontstaan kan Summa de gebruiker hiervoor volledig aansprakelijk stellen.
3. Indien er mogelijk sprake is van strafbare feiten zal hiervan aangifte worden gedaan bij de politie.

# 8 Slotbepalingen

## 8.1 Citeertitel

Dit reglement kan worden aangehaald als “Reglement gebruik ICT-faciliteiten Summa 2024”.

## 8.2 Medezeggenschap

De centrale studentenraad heeft ingestemd met dit reglement op 8 maart 2024, de ondernemingsraad op 1 februari 2024.

## 8.3 Ingangsdatum en wijziging

1. Dit reglement treedt in werking per 1 mei 2024 en heeft geen einddatum.
2. Summa heeft het recht om dit Reglement aan te passen waarbij wijzigingen niet eerder in werking treden dan na 30 dagen na bekendmaking van die wijziging(en).