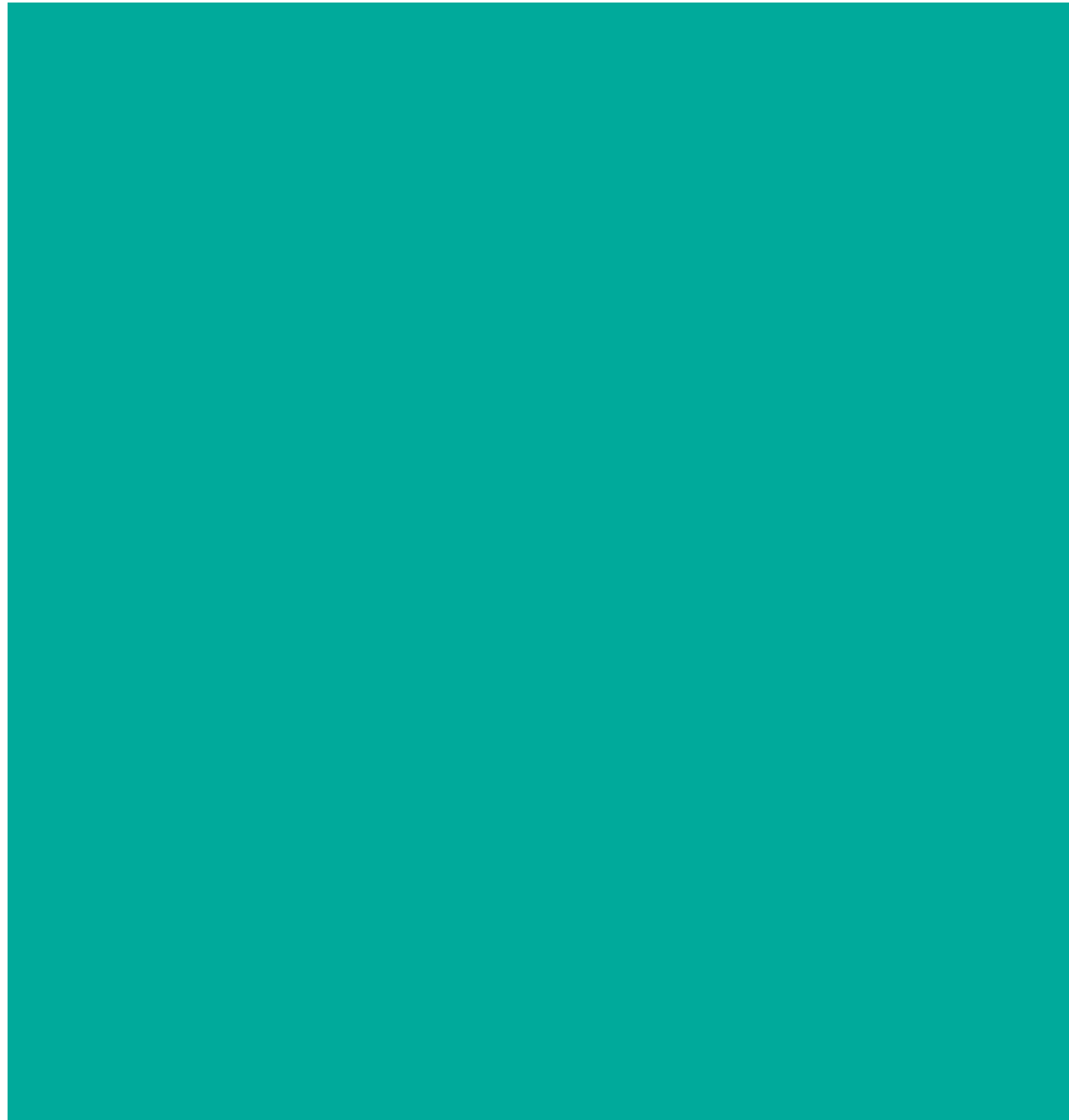

Gedragcode leerlingen/studenten ICT- en internetgebruik



Inhoud

Gedragcode leerlingen/studenten ICT- en internetgebruik.....	3
1. Inleiding.....	3
2. Gebruik van faciliteiten.....	3
3. Intellectueel eigendom en vertrouwelijke informatie.....	4
4. Beveiliging door Lentiz en door de leerling/student	4
5. Privégebruik en overlast	4
6. Monitoring door Lentiz	5
7. Procedure bij gericht onderzoek.....	5
8. Privacy van de leerling/student	6
9. Consequenties van overtreding	6
10. Slotbepalingen	7

Gedragscode leerlingen/studenten ICT- en internetgebruik

1. Inleiding

Jij als leerling/student van Lentiz mag op school internet gebruiken voor het volgen van onderwijs. Ook krijg je een school-mailbox en de mogelijkheid om je bestanden en studieresultaten op te slaan. Aan het gebruik hiervan zijn regels verbonden. Ben je minderjarig? Dan is deze gedragscode ook voor je ouders of verzorgers bedoeld.

2. Gebruik van faciliteiten

- 2.1. Je krijgt de beschikking over een computer (laptop of tablet) of toegang tot een netwerkaansluiting en e-mail, opslagruimte, printers en elektronische leeromgevingen voor het onderwijs. Dit zorgt ervoor dat je lessen kunt volgen, opdrachten, verslagen en scripties kunt maken, je resultaten kunt bijhouden, je bronnen kunt opzoeken en je contact kunt hebben met docenten en medeleerlingen/medestudenten.
- 2.2. Het gebruik van eigen apparatuur op school is toegestaan zolang je je houdt aan de regels van deze gedragscode. Het veranderen van instellingen in apparatuur en software die je van school krijgt is niet toegestaan.
- 2.3. Het op school aansluiten van eigen netwerkapparatuur waarmee de verbinding kan worden gedeeld met anderen is te allen tijde verboden.
- 2.4. Deze gedragscode geldt ook als jij als gast gebruik maakt van het netwerk van andere instellingen en je daarbij inlogt (eduroam) met de gegevens van je eigen Lentiz-school.
- 2.5. Voor het inloggen op de ICT-omgeving van Lentiz gebruik je je gebruikersnaam en wachtwoord, en soms ook een extra middel zoals een token of SMS. Je wachtwoord en token zijn alleen voor jou bestemd en mogen niet met anderen worden gedeeld.
- 2.6. Voor je wachtwoord en de manier waarop je toegang krijgt gelden bepaalde eisen. Informatie hierover vind je in het portaal MijnLentiz op de 'ICT-informatiesite leerlingen/studenten'.
- 2.7. Als er misbruik van je wachtwoord en/of token wordt gemaakt, wordt je toegang direct geblokkeerd. De directeur van je school wordt hierover op de hoogte gebracht.
- 2.8. Als je de computer en het netwerk wilt gebruiken om dingen te kopen of verkopen, mag dit alleen als de directeur van je school hiervoor schriftelijk toestemming heeft verleend.
- 2.9. Om de privacy en veiligheid van (mede)leerlingen/studenten en medewerkers van school te beschermen, mag je alleen opnames maken van lessen, gesprekken, en andere bijeenkomsten als hiervoor opdracht of schriftelijke toestemming is gegeven door de docent en/of schoolleiding.

3. Intellectueel eigendom en vertrouwelijke informatie

- 3.1. Je maakt geen misbruik van de apparatuur en software-licenties die door de school zijn aangeschaft.
- 3.2. Informatie die je van school krijgt, is en blijft van de school tenzij de directeur van je school de informatie aan je overdraagt.
- 3.3. Als je bij het uitvoeren van je schoolwerk toegang krijgt tot vertrouwelijke informatie of persoonsgegevens, moet je deze informatie strikt vertrouwelijk behandelen.
- 3.4. Is het bij het uitvoeren van je schooltaken nodig om vertrouwelijke informatie te gebruiken buiten de school (bijvoorbeeld per e-mail, op internet of eigen apparatuur)? Dan ga je zeer zorgvuldig om met die informatie.
- 3.5. Als de school extra regels heeft opgesteld voor het omgaan met apparatuur en software dan volg je deze regels ook op.

4. Beveiliging door Lentiz en door de leerling/student

- 4.1. Lentiz zorgt dat er steeds voldoende maatregelen worden genomen om de apparatuur, software en het netwerk te beveiligen tegen alle ongewenste activiteiten.
- 4.2. De school verwacht van jou als leerling/student dat jij serieuze stappen neemt om je eigen computer en andere apparatuur (zoals smartphones of tablets) te beveiligen. Je bent ook verantwoordelijk voor de opgeslagen gegevens op je eigen apparatuur.
- 4.3. Als je eigen apparatuur gebruikt verwachten we van je dat:
 - je gebruik maakt van een virusscanner;
 - je gebruik maakt van een moeilijk te raden wachtwoord of pincode en dat je deze regelmatig verandert;
 - je je apparatuur vergrendelt als je niet in de buurt bent zodat niemand bij de bestanden en gegevens kan;
 - je bij het weer in gebruik nemen van de apparatuur je deze ontgrendelt met een wachtwoord of pincode;
 - je steeds de nieuwste updates installeert op je apparatuur.

5. Privégebruik en overlast

- 5.1. Beperkt privégebruik van de faciliteiten is toegestaan, zolang het niemand stoort of overlast bezorgt. Ook mag het niet schadelijk zijn voor de apparatuur, software en het netwerk van school. Het is niet toegestaan om je school-mailadres te gebruiken voor gaming sites.
- 5.2. Met storend en overlast veroorzakend gebruik bedoelen we:
 - het bezoeken van pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud of het versturen van berichten met een dergelijke inhoud;
 - het versturen van berichten met een (seksueel) intimiderende inhoud of van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;

- het versturen van berichten aan grote aantallen ontvangers tegelijk;
- het versturen van kettingbrieven of het verspreiden van kwaadaardige software zoals virussen, worms, Trojaanse paarden en spyware;
- het gebruiken van filesharing- of streamingdiensten (zoals internetradio of Uitzending gemist) wanneer dit veel dataverkeer genereert, zodat het de beschikbaarheid van het netwerk in gevaar kan brengen;
- het downloaden van films, muziek, software en overig materiaal van een illegale bron of wanneer dit in strijd met rechten van de eigenaar(s);
- het verspreiden (uploaden) van films, muziek, software en overig materiaal naar derden zonder toestemming van de eigenaar(s).

6. Monitoring door Lentiz

- 6.1. We controleren het gebruik van apparatuur, software en het netwerk alleen om te zien of de regels van deze gedragscode worden nageleefd.
- 6.2. We proberen om illegaal gebruik van de apparatuur, software en het netwerk zoveel mogelijk tegen te gaan.
- 6.3. We verzamelen geautomatiseerd gegevens over het gebruik. Alleen de ICT-medewerkers kunnen dit inzien en geven dit als het nodig is alleen anoniem door aan de schoolleiding. De schoolleiding kan als het nodig is maatregelen nemen zoals het blokkeren van de toegang tot bepaalde software of de toegang vanaf een bepaald apparaat tot het netwerk.
- 6.4. Als jij overlast veroorzaakt door verkeerd gebruik van apparatuur, software en netwerk kan de schoolleiding besluiten om je toegang tot het netwerk af te sluiten. Als het kan zal je vooraf een waarschuwing krijgen zodat je de overlast kunt stoppen. Als dit vooraf niet kan, informeren we je direct na de afsluiting.

7. Procedure bij gericht onderzoek

- 7.1. Als er serieuze redenen zijn om te vermoeden dat er een ernstige overtreding van deze gedragscode plaatsvindt kan controle worden gedaan op de inhoud van je e-mails, bestanden, enzovoorts. Dit noemen we een gericht onderzoek.
- 7.2. Een gericht onderzoek wordt alleen uitgevoerd na schriftelijke opdracht van de directeur van je school. In de opdracht zullen de redenen worden vermeld waarom de toestemming wordt verleend. De Raad van Bestuur wordt geïnformeerd over het onderzoek en de resultaten.
- 7.3. Bij een gericht onderzoek wordt in eerste instantie gekeken naar het gebruik van de laptop, tablet, software en het netwerk. Als dit een bewijs oplevert, kan de school besluiten om de inhoud van communicatie of opgeslagen bestanden te raadplegen. Hiervoor wordt toestemming gevraagd aan de directeur van je school en de Raad van Bestuur. Als uit het onderzoek geen informatie komt die verder onderzocht moet worden, worden de gegevens van het onderzoek vernietigd.
- 7.4. We informeren jou en/of je ouders/verzorgers zo snel mogelijk. We vragen je om uitleg te geven over de aangetroffen gegevens. Alleen als het informeren zou leiden tot schade aan het onderzoek mogen we het informeren uitstellen.

- 7.5. Alleen in dringende gevallen of bij een duidelijk vermoeden van overtreding van deze gedragscode mogen medewerkers van afdeling I&A je inloggegevens inzien en toegang nemen tot je computer of account. In dat geval informeren we jou en/of je ouders/verzorgers achteraf.
- 7.6. Een gericht onderzoek naar de beveiliging en de juistheid van informatie op apparatuur mag door medewerkers van de afdeling I&A worden uitgevoerd zonder dat dit vooraf wordt bekendgemaakt. Dit mag alleen als daar concrete aanwijzingen voor zijn. De uitkomst van het onderzoek wordt alleen met jou gedeeld met het doel de beveiliging of de juiste opslag van gegevens op de apparatuur te verbeteren. Bij herhaling zal de procedure gevolgd worden zoals beschreven onder 7.2 en 7.3.

8. Privacy van de leerling/student

- 8.1. Lentiz houdt zich bij controles en onderzoeken aan de Algemene Verordening Gegevensbescherming en andere wetten die van toepassing zijn. Gegevens van onderzoeken worden extra beveiligd.
- 8.2. Verwerkt Lentiz bij een controle of onderzoek persoonsgegevens van jou? Dan mogen jij en/of je ouders/verzorgers op verzoek die persoonsgegevens inzien, laten corrigeren, of de verwerking van deze gegevens weigeren indien daar een gegronde reden voor is. De regels hiervoor zijn opgenomen in het 'Privacyreglement verwerking leerlinggegevens'.

9. Consequenties van overtreding

- 9.1. Als je je niet aan deze gedragscode of algemeen geldende wettelijke regels houdt, kan de directeur van je school disciplinaire maatregelen treffen. De maatregelen zijn afhankelijk van de aard en ernst van je overtreding. Mogelijke maatregelen zijn een waarschuwing, berisping, een tijdelijke afsluiting of beperking van toegang tot de computer, laptop, tablet en/of het netwerk (maximaal een jaar). In extreme gevallen kun je van school worden verwijderd.
- 9.2. Disciplinaire maatregelen (behalve een waarschuwing) kunnen alleen worden genomen nadat een medewerker van de afdeling I&A een overtreding heeft geconstateerd. Jij en/of je ouders/verzorgers krijgen in dat geval de gelegenheid een verklaring af te leggen.
- 9.3. Na de constatering van overlast kan tijdelijk je toegang tot een computer, laptop, tablet en/of het netwerk worden geblokkeerd. Deze blokkade duurt maximaal een week, of korter als de oorzaak van de overlast naar tevredenheid is weggenomen. Als na een week de overlast niet is weggenomen, kan de school besluiten tot een langere blokkade. Bij herhaling van de oorzaak kunnen disciplinaire maatregelen worden genomen.

10. Slotbepalingen

- 10.1. Deze gedragscode wordt driejaarlijks in opdracht van de Raad van Bestuur geëvalueerd en indien nodig aangepast. Wijzigingen worden bij het begin van een cursusjaar doorgevoerd, behalve in dringende gevallen of wanneer Lentiz door omstandigheden van buitenaf gedwongen is tot een snellere invoering.
- 10.2. Wijzigingen worden alleen ingevoerd nadat Platform MR om voorafgaand advies is gevraagd.
- 10.3. In gevallen waarin deze gedragscode niet voorziet, beslist de directeur en bij schooloverstijgende gevallen de Raad van Bestuur.

Deze gedragscode is na overleg met het Platform Medezeggenschap vastgesteld door de Raad van Bestuur op 5 november 2021 en vervangt alle voorgaande versies.