Protocol

voor het gebruik van e-mail, internet, en sociale media

voor het gebruik van camera- en videobeelden

Deze protocollen maken als BIJLAGES III en IV deel uit van het Privacyreglement van Het Amsterdams Lyceum

De schoolleiding van Het Amsterdams Lyceum heeft op grond van haar bevoegdheid ex art. 5 lid 4 van het Managementstatuut op 1 augustus 2018 de hierna volgende ***bijlages III en IV bij het Privacyreglement*** *vastgesteld na voorafgaande instemming van de afzonderlijke personeels- ouder- en leerlinggeledingen van de Medezeggenschapsraad o.g.v artt. 12 lid 1 sub m en n, 14 lid 2 sub f, respectievelijk 14 lid 3 sub d van de Wet medezeggenschap op scholen. De in bijlages opgenomen regelingen worden van kracht op de dag van vaststelling****.***

BIJLAGE III van het Privacyreglement van Het Amsterdams Lyceum: Protocol voor het gebruik van e-mail, internet, en sociale media

Artikel 1 Werkingssfeer van deze regeling, begrippen

1.1 Deze regeling beschrijft hoe bij Het Amsterdams Lyceum wordt omgegaan met informatie- en communicatietechnologie (hierna: ICT). Deze regeling omvat (gedrags)regels ten aanzien het gebruik van de ICT en geeft regels voor welke doeleinden en op welke wijze controle plaats vindt op dit gebruik.

1.2 Deze regeling geldt voor eenieder die ten behoeve van de school werkzaamheden verricht (medewerkers, maar bijvoorbeeld ook: stagiaires en vrijwilligers, hierna: *medewerkers*) of onderwijs volgt (leerlingen). Gezamenlijk worden zij in dit reglement ook aangeduid als: *gebruiker(s)*.

1.3 Elke nieuwe gebruiker wordt gewezen op de toepasselijkheid van deze regeling. Daarbij wordt aangegeven waar de volledige tekst van deze regeling geraadpleegd/ingezien kan worden. Alle medewerkers en leerlingen ontvangen eens per jaar een herinnering aan de geldende regels.

1.4 Voor zover de gebruikers thuis of elders gebruik maken van de ICT (bijvoorbeeld het e-mailadres van de school of de schoolwebsite) zijn de bepalingen van deze regeling eveneens van toepassing.

Artikel 2 Toegang tot en gebruik van de ICT

2.1 Het Amsterdams Lyceum geeft de gebruiker het recht op toegang tot de ICT (en de daarmee verbonden systemen en faciliteiten), maar behoudt zich het recht voor de toegang weer in te trekken.

2.2 De gebruiker dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen (zoals smartcards en tokens). Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet met anderen worden gedeeld. Bij een vermoeden van misbruik van een wachtwoord kan de ICT-beheerder per direct het betrokken account ontoegankelijk maken.

2.3 Het is gebruiker niet toegestaan om persoonsgegevens die gebruiker ter beschikking staan voor de uitoefening van zijn functie lokaal op te slaan (dus buiten het computernetwerk), noch op privé-apparatuur, tenzij daarvoor voorafgaande toestemming is verleend door diens leidinggevende en adequate waarborgen zijn getroffen voor de beveiliging van de persoonsgegevens.

Artikel 3 Gebruik van de ICT-apparatuur

3.1 De gebruiker dient zorgvuldig om te gaan met de ICT-apparatuur, zodat deze niet beschadigd raakt. De apparatuur dient in goede orde te worden achtergelaten. Eventuele schade of ontbreken van onderdelen dient direct gemeld te worden aan de ICT-afdeling.

3.2 Tijdens het gebruik van de ICT-apparatuur is het niet toegestaan etens- en drinkwaren te nuttigen.

3.3 Alleen de ICT-afdeling is bevoegd om apparatuur te ontkoppelen, verplaatsen of aan te sluiten aan het schoolnetwerk of aan apparatuur die aan het schoolnetwerk verbonden is.

3.4 De ICT-afdeling verleent alleen ondersteuning op apparatuur die door de ICT-afdeling is aangeschaft, aangesloten en geïnstalleerd.

3.5 Het gebruik van eigen opslagmedia (bijvoorbeeld: een USB-stick) van de gebruikers is toegestaan, mits onder de volgende voorwaarden:

a) voor het correct laten functioneren van het opslagmedium kan geen beroep worden gedaan op de ICT-afdeling;

b) de bestanden en programmatuur die op het opslagmedium staan moeten voldoen aan de voorwaarden zoals vastgelegd in dit reglement.

3.6 Het gebruik van eigen computerapparatuur (bijvoorbeeld laptops of tablets) is toegestaan onder de volgende voorwaarden:

a) Voorafgaand aan het gebruik is toestemming verleend door de leidinggevende en is contact opgenomen met de ICT-afdeling. Deze is bevoegd om, met opgaaf van redenen, de apparatuur niet toe te staan;

b) de gebruiker geeft de ICT-afdeling de gelegenheid om voorafgaand aan het gebruik maatregelen te treffen om de beheersbaarheid en de veiligheid te waarborgen;

c) het gebruik van de betreffende apparatuur moet voldoen aan de voorwaarden zoals vastgelegd in dit reglement.

Artikel 4 Toegang tot en gebruik van internet en e-mail

4.1 De toegang tot internet en bijbehorende faciliteiten, alsmede het e-mailsysteem en de bijbehorende mailbox met e-mailadres worden aan medewerkers voor gebruik in het kader van hun functies beschikbaar gesteld. Gebruik is derhalve gebonden aan taken die voortvloeien uit deze functies.

4.2 Het Amsterdams Lyceum behoudt zich het recht voor om de toegang tot bepaalde sites door middel van een filtersysteem te beperken.

4.3 Het versturen van e-mailberichten moet voldoen aan de volgende algemene voorwaarden:

a) de afzender wordt correct weergegeven;

b) duidelijke onderwerp aanduiding;

c) terughoudend omgaan met vertrouwelijke gegevens en gevoelige informatie.

4.4 Voor het verzenden en ontvangen van e-mail binnen de school wordt alleen gebruik gemaakt van de e-mailprogrammatuur die de school hiervoor beschikbaar stelt. Het gebruik van andere mailprogrammatuur is niet toegestaan.

4.5 Het verzenden van gegevens met gebruikmaking van Gmail, Hotmail, Dropbox, Whatsapp en WeTransfer kan leiden tot doorgifte van Persoonsgegevens buiten de EER, hetgeen slechts is toegestaan onder voorwaarden. Indien niet of niet langer aan deze voorwaarden wordt voldaan, kan Het Amsterdams Lyceum besluiten het gebruik van deze software door medewerkers te verbieden.

4.6 In geval van langdurige afwezigheid of het vermoeden van grove nalatigheid van de medewerker, doch uitsluitend als dit een zwaarwegende reden van bedrijfsbelang tot toegang oplevert, is Het Amsterdams Lyceum gerechtigd een vervanger van de medewerker of een leidinggevende toegang tot de bestanden of mailbox van de medewerker te verschaffen. Geen toegang wordt verleend tot als privé gemarkeerde mappen, als privé herkenbare mails, of mails verzonden naar dan wel afkomstig van een vertrouwenspersoon of bedrijfsarts.

Artikel 5 (On)verantwoord gebruik van de ICT

Verantwoord gebruik

5.1 Het gebruik van de ICT is primair verbonden met taken en bezigheden die voortvloeien uit het verstrekken of ontvangen van onderwijs en begeleiding. Als uitgangspunt geldt dat het gebruik van de ICT van de school ten dienste moet staan aan de werkzaamheden van het personeelslid of de opleiding van de leerling. Indien en voor zover sprake is van het verwerken van persoonsgegevens gebeurt dit met inachtneming van het Privacyreglement.

5.2 Medewerkers mogen de ICT beperkt, incidenteel en kortstondig gebruiken voor persoonlijke doeleinden, mits dit niet storend is voor de dagelijkse werkzaamheden of het systeem en mits hierbij wordt voldaan aan de verdere regels van deze regeling. Leerlingen mogen de ICT onder schooltijd in principe niet voor persoonlijke doeleinden gebruiken, tenzij zij daarvoor toestemming hebben gekregen.

5.3 Onverlet de plicht tot het melden van datalekken voor medewerkers zoals vastgelegd in art. 4 van het *Protocol Beveiligingsincidenten* [bijlage 1 van BIJLAGE XIII (*Handboek Datalekken*) van het *Privacyreglement*], melden gebruikers van de ICT systemen ieder vermoeden van misbruik van ICT en inbreuken op de beveiliging, van binnenuit of van buiten de school, alsmede door hen gesignaleerde zwakke plekken in de systemen. Hieronder vallen tevens inbreuken op de beveiliging die bij toeval worden ontdekt. Melding wordt gedaan bij de Functionaris Gegevensbescherming of de ICT-afdeling. In bijlage 1 bij dit Protocol (*Responsible Disclosure* Beleid) wordt deze verplichting nader toegelicht.

Onverantwoord gebruik

5.4 Het is niet toegestaan om de ICT zodanig te gebruiken dat het systeem- en/of de beveiliging opzettelijk worden aangetast.

5.5 Het is niet toegestaan zich toegang te verschaffen tot gegevens van andere gebruikers, tenzij met uitdrukkelijke toestemming van de betreffende gebruiker.

5.6 Het is niet toegestaan pogingen te ondernemen om het filtersysteem te omzeilen.

5.7 Het is in het bijzonder niet toegestaan om:

a) sites te bezoeken die pornografisch, racistisch, discriminerend, (seksueel) intimiderend, beledigend of aanstootgevend materiaal bevatten;

b) pornografisch, racistisch, discriminerend, (seksueel intimiderend, beledigend of aanstootgevend materiaal te bekijken of te downloaden of te verspreiden;

c) zich tot niet-openbare bronnen op het netwerk, internet of andere computernetwerken toegang te verschaffen en het bewust informatie waartoe men via de ICT oneigenlijk toegang heeft verkregen zonder toestemming te veranderen of te vernietigen;

d) bestanden te downloaden en/of op het computernetwerk of lokaal op een PC van de school te plaatsen die geen verband houden met studie en/of werk;

e) software en applicaties te downloaden en/of te installeren zonder voorafgaande toestemming van de ICT-afdeling;

f) niet-educatieve spelletjes te spelen;

g) anoniem of onder een fictieve naam via de ICT te communiceren;

h) op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende manier via de ICT te communiceren;

i) inkomende privé-berichten te genereren door het deelnemen aan niet-zakelijke nieuwsgroepen, abonnementen op e-zines, elektronisch winkelen, down- en uploaden van bestanden, nieuwsbrieven en dergelijke;

j) kettingmailberichten en andere berichten die verstopping veroorzaken of het werk van anderen verstoren te verzenden of door te sturen;

k) iemand lastig te vallen via de ICT;

l) het introduceren en verspreiden van computervirussen en andere software die de integriteit van de gegevens of de computerbeveiliging van de ICT kunnen beschadigen;

m) gebruik te maken van MSN Messenger en andere chatvoorzieningen.

5.8 Het is niet toegestaan om foto's, video's of ander materiaal van op school werkzame personen of leerlingen of andere bij de school betrokkenen via de ICT (daaronder ook begrepen: social media) te publiceren, tenzij dit gericht is op een aan het onderwijs gerelateerde doelstelling en de afgebeelde personen hebben aangegeven in te stemmen met dergelijke publicaties.

5.9 De gebruiker maakt geen inbreuk op de intellectuele eigendomsrechten van Het Amsterdams Lyceum en derden en respecteert licentieafspraken die van toepassing zijn voor de school.

5.10 Het is ook anderszins niet toegestaan om door middel van de ICT onrechtmatig of onethisch te handelen.

5.11 De schoolleiding kan de ICT-afdeling opdracht geven om na constatering ongeoorloofde data van het computernetwerk te verwijderen.

5.12 Voor medewerkers is het voor testdoeleinden toegestaan software lokaal te installeren die nodig is voor de werkzaamheden ten behoeve van school.

5.13 Als de gebruiker eraan twijfelt of een bepaald gebruik van ICT wel verantwoord is, dan overlegt hij daarover met de ICT-afdeling.

Artikel 6 Algemene uitgangspunten van controle op gebruik

6.1 Het Amsterdams Lyceum is als belanghebbende en verwerkingsverantwoordelijke gerechtigd om het gebruik van de ICT door medewerkers en leerlingen te controleren. De controle op gebruik van de ICT zal overeenkomstig deze regeling uitgevoerd worden. Als zich situaties voordoen waarin deze regeling niet voorziet, dan zal conform de Algemene Verordening Gegevensbescherming (AVG) gehandeld worden.

6.2 Als een lid van de schoolleiding merkt of erop geattendeerd wordt dat het ICT-gedrag van een medewerker niet binnen de kaders van dit reglement verloopt, wordt deze hierop direct gewezen en wordt een controle van zijn ICT-gebruik door bevoegde personen van de ICT-afdeling als mogelijkheid genoemd. Hiervan wordt melding gemaakt aan de rector.

6.3 Als een medewerker merkt dat het ICT-gedrag van een leerling niet binnen de kaders van dit reglement verloopt, dan spreekt deze de leerling hierop aan en meldt dit aan de afdelingsleider waaronder de leerling resorteert.

6.4 Gestreefd wordt naar een goede balans tussen enerzijds controle op het gebruik van de ICT en anderzijds de bescherming van de privacy van medewerkers en leerlingen.

6.5 Controle op het gebruik van de ICT zal waar mogelijk zoveel mogelijk geautomatiseerd plaatsvinden, waarbij in geval van verdachte berichten, het bericht geautomatiseerd wordt teruggezonden aan de verzender. Voor zover geautomatiseerde controle niet mogelijk, dan wel ontoereikend is, zal de controle op het gebruik van de ICT in beginsel steekproefsgewijs plaatsvinden.

6.6 In geval dat ten aanzien van een gebruiker, vanwege een concreet vermoeden van oneigenlijk gebruik, een gerichte controle is uitgevoerd, stelt de schoolleiding deze gebruiker daarvan zo spoedig mogelijk nadat de controle heeft plaatsgevonden op de hoogte.

6.7 Persoonsgegevens met betrekking tot het gebruik van ICT worden niet langer bewaard dan noodzakelijk, met een bewaartermijn van maximaal 6 maanden. Onder omstandigheden kan een langere bewaartermijn gerechtvaardigd zijn. In dat geval zal de verwerking worden gemeld bij de Autoriteit Persoonsgegevens.

6.8 Privémail/-gebruik (voorzien van het label ‘persoonlijk’) wordt zoveel mogelijk ontzien van controle.

6.9 Elektronische informatie- en communicatieberichten van vertrouwenspersonen en andere medewerkers met een vertrouwensfunctie, gecommuniceerd in het kader van hun functie, zijn uitgesloten van inhoudelijke controle.

6.10 De schoolleiding treft voorzieningen voor de positie en de integriteit van de ICT-afdeling. De medewerkers van de ICT-afdeling hebben een geheimhoudingsplicht die inhoudt dat ten aanzien van de verzamelde en voor hen inzichtelijke informatie strikte geheimhouding betracht dient te worden.

Artikel 7 Doeleinden van controle

7.1 De controle op persoonsgegevens bij gebruik van de ICT vindt slechts plaats met als doel:
- a) het tegengaan van onverantwoord en ontoelaatbaar gebruik;
- b) de naleving van het Privacyreglement;
- c) het bewaken van de voortgang van werkzaamheden;
- d) het vastleggen van bewijs en/of archief;
- e) de systeem- en netwerkbeveiliging;
- f) de kosten- en capaciteitsbeheersing.

7.2 Onder 'onverantwoord en ontoelaatbaar gebruik' als bedoeld in artikel 7.1 wordt begrepen: het onverantwoord gebruik als opgenomen in artikel 5.4 tot en met 5.13.

7.3 Onder 'bewaking van de voortgang van de werkzaamheden' als bedoeld in artikel 7.1 wordt begrepen: controle op de inhoud van zakelijke e-mails van medewerkers voor wie het communiceren per e-mail rechtstreeks met de te verrichten taken verband houdt. Middels deze controle kan de voortgang van de werkzaamheden worden gegarandeerd bij ziekte of afwezigheid van de medewerker.

7.4 Onder 'vastleggen van bewijs en/of archief' als bedoeld in artikel 7.1 wordt begrepen: het maken van kopieën van e-mails vanuit de behoefte aan bewijs voor zakelijke transacties en dossiervorming (al dan niet met het oog op het voeren van juridische procedures).

7.5 Onder 'systeem- en netwerkbeveiliging' als bedoeld in artikel 7.1 wordt begrepen: controle op het e-mail- en internetgebruik ter voorkoming van systeemaanvallen door onder andere virussen, trojans of andere schadelijke programma's.

7.6 Onder 'kosten- en capaciteitsbeheersing' als bedoeld in artikel 7.1 wordt begrepen: controle op het e-mail- en internetgebruik ter inventarisering en/of beheersing van de kosten die gemoeid zijn met het gebruik van de ICT.

Artikel 8 Specifieke uitgangspunten van controle op gebruik

8.1 In het kader van de controle op de gebruikers voor het doel als bedoeld in artikel 7.1a geldt dat:

a) controle op de naleving van de regels vindt in beginsel geautomatiseerd en steekproefsgewijs plaats;
b) indien er een concreet vermoeden is dat een gebruiker de regels, waarvan de naleving wordt gecontroleerd, overtreedt, vindt zo nodig een in tijd en omvang zo beperkt mogelijke gerichte controle op persoonsniveau plaats;
c) daarbij worden in eerste instantie de berichten en/of het surfgedrag gescreend op (onder andere) verdachte afzender(s), bestemming, website, verdacht onderwerp, verdachte zoekopdracht, verboden woord in de inhoud of verboden extensies van de bijlage(n);
d) Vervolgens worden de berichten, waarvan aannemelijk is dat het regulier verkeer betreft of waartegen ook overigens geen bedenkingen bestaan, ongeopend doorgezonden (bij originelen) of vernietigd (kopieën);
e) de overgebleven berichten kunnen worden geopend voor nader inhoudelijk onderzoek.

8.2 In het kader van de controle voor het doel als bedoeld in artikel 7.1 b geldt dat slechts berichten worden verwerkt die rechtstreeks verband houden met uitvoering van de te verrichten taken door het personeelslid.

8.3 In het kader van de controle voor het doel als bedoeld in artikel 7.1 c geldt dat slechts de e-mailverkeersgegevens en inhoud van de berichten wordt verwerkt.

8.4 In het kader van de controle voor het doel als bedoeld in artikel 7.1 d geldt dat slechts zakelijke berichten worden verwerkt voor zover deze kunnen dienen als bewijs van zakelijke transacties en dossiervorming.

8.5 In het kader van de controle voor het doel als bedoeld in artikel 7.1 e geldt dat:
a) de controle geheel geautomatiseerd plaatsvindt;
b) een gevonden besmet bericht/bestand op een aparte locatie bewaard wordt voor nader onderzoek en eventuele herstelwerkzaamheden.

8.6 In het kader van de controle voor het doel als bedoeld in artikel 7.1 e geldt dat slechts de
a) e-mailverkeersgegevens en inhoud (en bijlagen) van berichten met een verdachte inhoud worden gecontroleerd;
b) internetverkeersgegevens en inhoud van berichten met een verdachte inhoud worden gecontroleerd.

8.7 In het kader van de controle voor het doel als bedoeld in artikel 7.1 f geldt dat de controle van het e-mail- en internetverkeer beperkt blijft tot de verkeersgegevens.

8.8 In het kader van de controle voor het doel als bedoeld in artikel 7.1 f geldt dat slechts de
a) e-mailverkeersgegevens over tijd, hoeveelheid, omvang en dergelijke worden verwerkt;
b) internetverkeersgegevens over tijd en dergelijke worden verwerkt.

Artikel 9 Gebruik van social media

9.1 Onder social media wordt verstaan alle huidige en toekomstige online platformen waarbij de gebruikers de inhoud verzorgen.

9.2 Indien social media voor onderwijsdoeleinden worden gebruikt dient dit – met het oog op de bescherming van leerlinggegevens - plaats te vinden conform het Privacyreglement.

9.3 Voor het overig gebruik geldt dat dit in eigen tijd dient plaats te vinden. Dat geldt ook voor het gebruik van social media door middel van smartphones of tablets.

9.4 Voor zover de gebruikers (leerlingen, medewerkers of derden) aan de school verbonden zijn, geldt in algemene zin dat zich niet op social media zullen uitlaten op een wijze die schadelijk kan zijn voor Het Amsterdams Lyceum.

Artikel 10 Richtlijnen voor het gebruik van social media

10.1 Voor zover de gebruiker op social media uitingen doet die in relatie staan tot Het Amsterdams Lyceum geeft hij steeds duidelijk aan in welke relatie (bijvoorbeeld: personeelslid of leerling) hij staat tot de school.

10.2 De gebruiker plaatst op social media geen content met een onverantwoorde inhoud.

10.3 De gebruiker deelt op social media geen interne- of bedrijfsvertrouwelijke informatie over de school.

10.4 De gebruiker deelt geen persoonsgegevens van personeel of leerlingen waartoe hij uit hoofde van zijn functie toegang heeft.

10.5 De gebruiker laat zich op social media niet negatief of anderszins ongepast uit over de school, over collega's, over medewerkers en/of over (mede-)leerlingen.

10.6 De gebruiker plaatst op social media niet zonder toestemming foto's of andere afbeeldingen van de school en/of aan de school verbonden personen.

10.7 De gebruiker plaatst op social media geen content namens Het Amsterdams Lyceum, tenzij hij daarvoor toestemming heeft gekregen.

10.8 In zijn algemeenheid geldt dat de gebruiker op social media geen content zal plaatsen of zich anderszins zal gedragen op een wijze die de school schade kan toebrengen.

Artikel 11 Richtlijnen voor contacten door middel van ICT

11.1 Onderling privé-contact tussen medewerkers en leerlingen, binnen dan wel buiten schooltijd, door middel van e-mail en smartphones (bijvoorbeeld via Whatsapp) is in beginsel verboden.

11.2 Een uitzondering kan aan de orde zijn ten aanzien van leerlingen die speciale begeleiding op afstand nodig hebben, bijvoorbeeld in geval van ziekte. Een dergelijk contact mag alleen betrekking hebben op onderwijsgerelateerde zaken (bijvoorbeeld kennisoverdracht, afstemming

huiswerk, ondersteuning) en dient vooraf gemeld te zijn aan de rector. Het personeelslid mag het contact met de leerling uitsluitend onderhouden via het e-mailadres van de school.

11.3 Onderling contact tussen medewerkers over een leerling is uitsluitend toegestaan in verband met onderwijsgerelateerde zaken en mag uitsluitend verlopen via het e-mailadres van de school.

11.4 Het is medewerkers niet toegestaan persoonsgegevens van leerlingen op te slaan op servers die niet worden gebruikt of beheerd door de school of lokaal op de eigen PC respectievelijk tablet of smartphone, dan wel op eigen gegevensdragers.

11.5 Gewisselde (e-mail)correspondentie wordt maandelijks door de betrokken docenten vernietigd dan wel – indien de informatie relevant is voor de begeleiding van de leerling - verplaatst en opgeslagen in het leerlingvolgsysteem van Het Amsterdams Lyceum.

Artikel 12 Disciplinaire maatregelen bij leerlingen

12.1 Indien door de schoolleiding wordt vastgesteld dat een leerling onverantwoordelijk gebruik heeft gemaakt van de ICT, kan de schoolleiding – afhankelijk van de aard en de ernst van het onverantwoorde gebruik – overgaan tot:

a) het tijdelijk uitsluiten van inlogmogelijkheden voor de betrokken leerling;
b) het melden van dit gedrag en de consequenties aan de ouder(s)/verzorger(s); en/of
c) het opleggen van een straf/maatregel.

Artikel 13 Disciplinaire maatregelen bij medewerkers

Indien door de schoolleiding wordt vastgesteld dat een personeelslid onverantwoordelijk gebruik heeft gemaakt van de ICT, kan de schoolleiding - afhankelijk van de aard en de ernst van het incident – maatregelen treffen, zoals een berisping, schorsing of ontslag.

Bijlage 1 als bedoeld in art. 5.3 van:

Protocol voor het gebruik van e-mail, internet, en sociale media

[BIJLAGE III van het Privacyreglement van Het Amsterdams Lyceum]

Bewerkte bron:

Responsible Disclosure Beleid

Responsible Disclosure is de overkoepelende term voor de praktijk van het verantwoord melden van tijdens het gebruik van de ICT aangetroffen beveiligingsproblemen. Hierbij worden afspraken gehanteerd die er doorgaans op neerkomen dat de melder de ontdekking niet deelt met derden totdat het lek verholpen is, en de getroffen partij geen (juridische) stappen tegen de melder zal ondernemen.

De onderstaande gedragscode voor gebruikers omvat het beleid van de school voor het melden van vermoedelijke beveiligingsproblemen en het verantwoord openbaar maken daarvan.

Vooraf:

Op Het Amsterdams Lyceum vinden wij de veiligheid van de ICT, onze informatiesystemen (internet en bijbehorende hardware en software), erg belangrijk. Ondanks onze zorg voor de beveiliging van deze systemen kan het gebeuren dat er toch een zwakke plek (kwetsbaarheid) voorkomt. Als de gebruiker een zwakke plek in één van onze systemen heeft gevonden, dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag samenwerken op dit punt om onze gebruikers zelf en onze systemen beter te kunnen beschermen.

Echter een waarschuwing is wel op zijn plaats. Ons beleid op het gebied van *Responsible Disclosure* is geen uitnodiging om ons netwerk uitgebreid te scannen om zwakke plekken te ontdekken. Er bestaat een kans dat men tijdens zo'n onderzoek handeling uitvoert die in strijd zijn met strafrechtelijke bepalingen. Ook als de schoolleiding geen juridische stappen onderneemt, sluit dit niet uit dat er in dat geval een strafrechtelijk onderzoek wordt gehouden.

Van de gebruikers wordt gevraagd:

- De bevindingen ten aanzien van de kwetsbaarheid direct per email of telefonisch te melden aan de ICT-afdeling of de Functionaris Gegevensbescherming.
- De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om de zwakke plek aan te tonen of (persoons)gegevens van derden in te kijken, te verwijderen of aan te passen.
- De kwetsbaarheid niet met anderen te delen of anderszins openbaar te maken totdat deze is verholpen en alle (vertrouwelijke) gegevens die zijn verkregen via de zwakke plek direct na het verhelpen hiervan te verwijderen.

- Geen enkele vorm van publiciteit te zoeken over de aangetroffen kwetsbaarheid buiten medeweten van de rector van de school.
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden.
- Voldoende informatie te geven om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

Aan de melder wordt toegezegd:

- Wij reageren binnen drie dagen op de melding met een beoordeling van de melding en een verwachte datum voor een oplossing.
- Als de gebruiker zich aan de hierboven vermelde voorwaarden heeft gehouden zullen geen (juridische) stappen worden ondernemen betreffende de melding.
- Wij behandelen de melding vertrouwelijk en zullen de persoonlijke gegevens van de meldende gebruiker niet zonder diens toestemming met derden delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk.
- Voor het onderzoek kan aan de melder een beloning worden toegekend. Daartoe bestaat echter geen verplichting. De vorm van deze beloning staat ook niet van tevoren vast en hangt af van de zorgvuldigheid van het onderzoek, de kwaliteit van de melding en de ernst van de gemelde kwetsbaarheid.
- Wij houden de melder op de hoogte van de voortgang van het verhelpen van de kwetsbaarheid.
- In berichtgeving over het gemelde probleem wordt indien gewenst, de naam van de melder vermeld als de ontdekker. Wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

Bijlage IV van het Privacyreglement van Het Amsterdams Lyceum
Protocol gebruik van camera- en videobeelden

Artikel 1 Doel van camera- en video-opnames

Het maken van (digitale)opnames heeft ten doel:

- zorgdragen voor beveiliging om ongewenst gedrag (waaronder, maar niet uitsluitend: diefstal, vandalisme en pestgedrag) te voorkomen en in voorkomende gevallen te kunnen signaleren en vastleggen.
- het begeleiden en coachen van medewerkers, in het bijzonder maar niet uitsluitend onderwijzend personeel in lessituaties.

Artikel 2 Begripsbepaling

2.1 camera's: het betreft camera's die bedoeld zijn voor algemeen toezicht;
2.2 camerasysteem: het geheel van camera's, monitoren, opnameapparatuur, verbindingskasten, glasvezelverbindingen en bevestigingen;
2.3 video-opnames: camera-opnames met als doel begeleiding en coaching van personeel;
2.4 beheer: zorg voor de continuïteit van het cameratoezicht;
2.5 Functionaris Gegevensbescherming: degene die is belast met het beheer van het camerasysteem;
2.6 beeldinformatie: de door het camerasysteem verkregen en geregistreerde filmbeelden.

Artikel 3 Plaats- en tijdbepaling cameratoezicht en video-opnames

3.1 Cameratoezicht vindt plaats op het schoolterrein van Het Amsterdams Lyceum aan de adressen Valeriusplein 15 en Olympiaplein 6 te Amsterdam. Binnen de school vindt cameratoezicht plaats bij alle toegangsdeuren, in gangen en trappenhuizen, in de kluisjesruimte en de leerlingenverblijfsruimte. De camera's zijn 24/7 operationeel, maar worden tijdens de openingsuren in de publieksruimtes in principe uitgeschakeld.
3.2 Video-opnames worden gemaakt in lessituaties, op incidentele basis en steeds tevoren aangekondigd. Over het moment waarop de opnames worden gemaakt worden de betrokken leerlingen en hun ouders/verzorgers vooraf geïnformeerd.
3.3 Indien een leerling en/of zijn ouders bezwaar hebben tegen de opnames die met het oog op begeleiding en coaching van personeel worden gemaakt, dan zal de school ervoor zorgen dat de leerling tijdens de opnames een dusdanige plek krijgt in de klas dat deze niet in beeld komt.

Artikel 4 Taken, verantwoordelijkheden en beveiliging

4.1 Het cameratoezicht en het maken van video-opnames geschiedt onder verantwoordelijkheid van de schoolleiding.

4.2 Degene die belast is met het beheer van het camerasysteem is de Functionaris Gegevensbescherming (FG).

4.3 Bevoegd tot het bedienen van het camerasysteem en het bekijken van de beelden zijn de leden van de schoolleiding, de conciërges en de systeembeheerder.

4.4 Degenen die toegang hebben tot de camera en videobeelden zullen daarmee strikt vertrouwelijk omgaan. Zij zullen geheimhouding betrachten (zie art. 4.3 van het Privacyreglement).

4.5 Er zijn passende technische en organisatorische maatregelen getroffen ter beveiliging van de camerabeelden en het camerasysteem.

Artikel 5 Kenbaarheid

5.1 Het cameratoezicht wordt kenbaar gemaakt door middel van stickers op de plaatsen waar cameratoezicht plaatsvindt en bij de ingang van het terrein.

5.2 Video-opnames met als doel begeleiding en coaching worden uitsluitend gemaakt nadat daarvoor uitdrukkelijke toestemming van de betrokken medewerkers is verkregen en de betrokken leerlingen vooraf zijn geïnformeerd.

5.3 Alle medewerkers en leerlingen worden geïnformeerd over dit protocol.

5.4 Voor betrokkenen (niet zijnde medewerkers of leerlingen) ligt het protocol ter inzage bij de administratie van de school.

Artikel 6 Doelbinding, zorgvuldigheid, bewaartermijnen en rechten van betrokkenen

6.1 De geregistreerde camera- en videobeelden worden uitsluitend gebruikt voor de doelen die in dit protocol zijn verwoord.

6.2 Het gebruik van de camera- en videobeelden zal niet verder gaan dan strikt noodzakelijk is voor het doel waarvoor het toezicht is ingesteld.

6.3 De camerabeelden die gemaakt zijn met het oog op de veiligheid van de school worden vier weken nadat deze zijn gemaakt, verwijderd. De camerabeelden mogen langer bewaard worden in het kader van een wettelijke bewaarplicht of als dat noodzakelijk is voor de afhandeling van geconstateerde incidenten. Zodra het incident is afgehandeld, worden de beelden vernietigd.

6.4 Videobeelden die zijn gemaakt met het oog op begeleiding en coaching van personeel, worden bewaard gedurende het begeleidingstraject. Na afronding van het begeleidingstraject of zoveel eerder als daarom door de medewerker wordt verzocht, worden de beelden vernietigd.

6.5 De betrokkene van wie beelden zijn vastgelegd heeft recht van inzage, recht op rectificatie, recht op het wissen en recht op beperking van verwerking van gegevens conform artikel 6 van het Privacyreglement.

Artikel 7 Heimelijk cameratoezicht

7.1 Heimelijk cameratoezicht kan worden ingezet indien er sprake is van een serieus en concreet vermoeden van diefstal, c.q. andere onrechtmatigheden en de schoolleiding er niet in is geslaagd om met behulp van minder vergaande middelen – waaronder het reguliere cameratoezicht – tot resultaten te komen.

7.2 Het heimelijk cameratoezicht wordt in duur en omvang zo beperkt mogelijk gehouden.

7.3 Het heimelijk cameratoezicht zal zich niet uitstrekken tot plaatsen waar de privacy van de betrokkenen onder alle omstandigheden gewaarborgd dient te zijn, waaronder in ieder geval doch niet uitsluitend, de was-en toiletruimten, de kamers van de schoolleiding, de vertrouwenspersoon e.d.