PROTOCOL PC-gebruik van IRIS

Regeling gebruik computernetwerk/e-mail- en Internetgebruik voor medewerk(st)ers en leerlingen van IRIS, een en ander mede in het kader van de Wet Bescherming Persoonsgegevens.

Doel van het protocol:

Het protocol bevat regels en afspraken omtrent computergebruik door medewerk(st)ers en leerlingen in IRIS en omtrent de wijze waarop IRIS omgaat met het registeren, verzamelen en monitoren van tot een persoon herleidbare data omtrent e-mail- en Internetgebruik. Doelstelling hiervan is een goede balans te vinden tussen een verantwoord gebruik van Internet en e-mail en bescherming van de privacy van werknemers en leerlingen op de werkplek c.q. op de studieplek.

Artikel 1. Werkingssfeer

Deze regeling geldt voor een ieder die voor IRIS werkzaam is dan wel als leerling of cursist is ingeschreven bij de school.

Artikel 2. Algemene uitgangspunten

1. Gegevens die tot een persoon herleidbaar zijn zullen niet worden geregistreerd, verzameld, gecontroleerd, gecombineerd dan wel bewerkt, anders dan in dit protocol is afgesproken.

2. Persoonsgegevens zullen alleen gebruikt worden voor het doel waarvoor ze verzameld zijn.

3. Het registreren van gegevens die tot een persoon herleidbaar zijn wordt tot het minimum beperkt. Hierbij wordt gestreefd naar een maximale bescherming van de privacy van werknemers op de werkplek.

4. Indien zulks uit een oogpunt van noodzakelijk te verrichten werkzaamheden onvermijdelijk is, is het aan het beheer van het netwerk toegestaan om persoonlijke data van gebruikers tijdelijk ontoegankelijk te maken.

Artikel 3. Algemene bepalingen t.a.v. leerlingen

1. Ieder die als leerling staat ingeschreven bij de Leerlingenadministratie van IRIS heeft toegang tot het computernetwerk. De voor het gebruik noodzakelijke gebruikersnaam, wachtwoord en mailadres worden door de Facilitaire Dienst verstrekt.

2. De eerste keer dat de leerling gebruik maakt van het computernetwerk zal dat worden beschouwd als de totstandkoming van een overeenkomst tussen IRIS en leerling m.b.t. het computergebruik, waarbij de leerling instemt met de in dit protocol verwoorde regels en afspraken.

3. Het recht om gebruik te maken van het computernetwerk vervalt zodra iemand niet meer ingeschreven staat bij IRIS.

4. Het computernetwerk kan door leerlingen worden gebruikt op daartoe ingerichte werkplekken.

5. Het is niet toegestaan te eten en/of te drinken nabij computers.

6. Leerlingen dienen zich te houden aan de aanwijzingen van de personeelsleden van IRIS.

Artikel 4. E-mailgebruik

1. Werknemers en leerlingen zijn gerechtigd het emailsysteem kortstondig voor niet-zakelijk (persoonlijk) verkeer te gebruiken voor het ontvangen en versturen van persoonlijke mailberichten zowel intern als extern, mits dit niet storend is voor hun dagelijkse werkzaamheden of voor anderen.

2. Het recht van de werknemer en de leerling om persoonlijke mailberichten te ontvangen en versturen is gebonden aan de voorwaarde dat het niet is toegestaan dreigende, intimiderende, seksueel getinte, pesterige, treiterende dan wel racistische of discriminerende berichten te versturen dan wel berichten te versturen die een gewelddadig of beledigend karakter hebben.

3. IRIS zal niet de inhoud van zowel persoonlijke als zakelijke mailberichten lezen. Gegevens omtrent het aantal mails, de mailadressen en andere data hieromtrent worden wel geregistreerd, voor zover zulks vereist is i.v.m. wettelijke of contractuele verplichtingen vanuit het optreden als provider (Telecommunicatiewet). Dit laat onverlet dat controles op incidentele basis (steekproef) of vanwege een zwaarwichtige reden kunnen plaats vinden. Hiervan wordt melding gemaakt bij de functionaris bescherming persoonsgegevens.

4. De normale gedragsregels, zoals die gelden voor schriftelijke correspondentie (zoals correct taalgebruik) zijn ook van toepassing op e-mail en andere toepassingen (zoals nieuwsgroepen).

Artikel 5. Internetgebruik

1. Werknemers en leerlingen zijn gerechtigd kortstondig het Internetsysteem voor niet- zakelijk resp. niet-onderwijsgebonden (persoonlijk) verkeer te gebruiken, mits dit niet storend is voor hun dagelijkse werkzaamheden of voor anderen.

2. IRIS zal geen persoonsgegevens over Internetgebruik, zoals tijdsbesteding en bezochte sites, registeren en/of controleren, tenzij zulks voortvloeit uit verplichtingen als provider op grond van de Telecommunicatiewet. Dit laat onverlet dat controles op incidentele basis (steekproef) of vanwege een zwaarwichtige reden kunnen plaats vinden. Hiervan wordt melding gemaakt bij de functionaris bescherming persoonsgegevens.

3. IRIS behoudt zich het recht voor om de toegang tot bepaalde sites te beperken. Met name sites met een pornografische, racistische, discriminerende of een op entertainment gerichte inhoud zullen worden geweerd.

4. IRIS kan het recht op gebruik van (een deel van) Internet toestaan, maar ook altijd weer intrekken. Zonder dat recht is gebruik van (een deel van) Internet niet toegestaan.

5. Het raadplegen van nieuwsgroepen en sites die gericht zijn op discriminatie, racisme, pornografie, beledigingen en extreme uitingen die aanstootgevend kunnen zijn dan wel die oproepen tot geweld, zijn verboden.

Artikel 6. Gedragsregels

De infrastructuur voor elektronische communicatie kent een eigen vorm van kwetsbaarheid, en een eigen vorm van beveiliging. Deze vraagt om speciale aandacht op tenminste de volgende punten:

1. Algemeen
   - gebruikersnaam (inlognaam) en wachtwoord zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven; de geregistreerde gebruiker is verantwoordelijk voor alle acties die met behulp van zijn/haar gebruikersnaam worden uitgevoerd.
   - het downloaden of kopiëren van software en applicaties is niet toegestaan, tenzij vooraf schriftelijke toestemming is verleend door de verantwoordelijke of de beheerder. Deze toestemming wordt alleen verleend als wordt voldaan aan de geldende rechten en eventuele licenties worden betaald. Gedownloade software en applicaties moeten op virussen zijn gescand voor gebruik; er mag niet gehandeld worden in strijd met auteursrechtelijke voorschriften.

- vertrouwelijke gegevens en bedrijfsgevoelige informatie mogen niet zonder toestemming buiten de organisatie worden verstuurd.
- het is niet toegestaan op enige wijze lessen of anderszins ingeroosterde activiteiten te beperken of te hinderen. Tijdens deze lessen en activiteiten is in de betreffende ruimte vrij practicum niet mogelijk.
- de gebruiker wordt aanbevolen zelf zorg te dragen voor het maken van een eigen veiligheidskopie.
- IRIS is niet aansprakelijk voor verlies van data of voor de schade, die de gebruiker lijdt in geval van (tijdelijke) onbereikbaarheid van de bestandsopslag of voor schade, welke de gebruiker mogelijk lijdt als gevolg van het (tijdelijk) niet bereikbaar zijn van het computernetwerk.
- het is niet toegestaan zonder toestemming andere computers en/of netwerken binnen te dringen (ook wel “hacken” genoemd). Dit geldt voor systemen binnen en buiten de school.
- IRIS is niet aansprakelijk voor mogelijke onjuiste adviezen die haar medewerkers aan de gebruikers geven, dan wel verkeerde interpretaties door de gebruiker van de gegeven adviezen, noch voor eventueel hieruit voortvloeiende schade, waaronder gevolgschade.
- IRIS is niet aansprakelijk/niet verantwoordelijk voor verlies van data veroorzaakt door technische storingen bij de school, dan wel andere interne of externe storing indien dit is veroorzaakt door overmacht. De school raadt gebruikers aan een back-up exemplaar van alle bestanden te bewaren. De gebruiker vrijwaart de school van elke aansprakelijkheid die mogelijk zou kunnen ontstaan door informatie en activiteiten die de gebruiker op het computernetwerk en/of het Internet plaatst en/of ontplooit. De gebruiker wordt expliciet gewezen op het feit dat overtredingen van buitenlandse wetten en regels (met name die van de USA) met het Internet en e-mail gebruik, kunnen leiden tot ernstige strafrechtelijke gevolgen bij bezoek aan landen waar deze wetten en regels van toepassing zijn.

2. Het is niet toegestaan inkomende privé-berichten te genereren door deel te nemen aan niet-zakelijke nieuwsgroepen, abonnementen op E-zines, nieuwsbrieven en dergelijke; onbedoelde inbreuken op beveiliging, van binnenuit of vanuit de buitenwereld, dienen aan de ICT-manager (FADI) gemeld te worden.

3. Het is in het bijzonder niet toegestaan om op Internet:

   - sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten, dan wel die oproepen tot geweld;
   - materiaal te bekijken of te downloaden dat pornografisch, racistisch, discriminerend, beledigend of aanstootgevend is dan wel oproept tot geweld;
   - films en muziek te downloaden en/of op te slaan;
   - spelletjes te downloaden of uit te voeren, te winkelen, te gokken, deel te nemen aan kansspelen en/of chat-/babbelboxen te bezoeken, tenzij zulks past in het kader van zakelijke- of onderwijsactiviteiten (zoals b.v. ELO);
   - zich ongeoorloofd toegang te verschaffen tot niet openbare bronnen op het Internet;
   - opzettelijk informatie - waartoe men via Internet toegang heeft verkregen - zonder toestemming te veranderen of te vernietigen;
   - indien ongevraagd informatie van deze aard wordt aangeboden, dient dat aan de ICT-manager (FADI) gemeld te worden;

4. Het is bovendien niet toegestaan om door middel van e-mail:

   - berichten anoniem of onder een fictieve naam te versturen; dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten en kettingmailberichten te verzenden of door te sturen ongeacht of de ontvanger deze wilde ontvangen;
   - iemand elektronisch lastig te vallen zoals het in hoge frequentie en/of grote omvang berichten versturen in de vorm van bijvoorbeeld bulkmail, junkmail, mailbombing, of welke vorm dan ook.

5. Het is niet toegestaan:

softwareprogramma’s/scripts/commando’s te gebruiken, of anderszins activiteiten te ondernemen, welke de beschikbaarstelling van het netwerk aan andere gebruikers op een nadelige wijze zal kunnen beïnvloeden;

- processen/programma's op de systemen van IRIS te laten lopen als er geen directe verbinding met het systeem is;
- processen/programma's op de systemen van IRIS te installeren zonder uitdrukkelijke schriftelijke toestemming van IRIS;
- buiten de voorgeschreven wijze om gebruik te maken van het netwerk;
- eigen software te gebruiken (in verband met het gevaar van virussen);
- gebruik te maken van het netwerk zonder op de gebruikelijke manier in te loggen;
- zonder toestemming van de rechtmatige gebruiker mail te verzenden, waarin in de header iemand anders zijn verzend of reply-adres wordt vermeld.

6. IRIS is gerechtigd zonder voorafgaande bekendmaking het computernetwerk (tijdelijk) buiten gebruik te stellen en/of het gebruik ervan te beperken voor zover dit noodzakelijk is voor het redelijkerwijs benodigde onderhoud en de veiligheid van de systemen.

Artikel 7. Controle

1. Om de veiligheid van het netwerk te waarborgen en toe te zien op een zorgvuldig gebruik overeenkomstig deze regeling, worden van tijd tot tijd controles uitgevoerd. Hiernaast wordt toegezien op de technische integriteit en beschikbaarheid van de infrastructuur en diensten.
   Het toezicht op het gebruik zal bestaan uit het steekproefsgewijs controleren van het gebruik van Internet en e-mail verkeer (tijdsbesteding, sites die bezocht worden). Daartoe kunnen anonieme lijsten van bezochte Internetsites en van verstuurde e-mails worden uitgedraaid.

2. Binnenkomend Internet- en e-mailverkeer wordt zo goed mogelijk gecontroleerd op virussen en soortgelijk ongerief. Mocht blijken dat een e-mailbericht een virus bevat, dan kan dat automatisch tegengehouden worden en dan worden de verzender en ontvanger daarover ingelicht. Indien desondanks een e-mail wordt ontvangen dat mogelijk een virus bevat, dan dient de ontvanger onverwijld contact op te nemen met het hoofd technisch beheer.

3. Indien mocht blijken dat in strijd met deze regeling wordt gehandeld of indien daarvoor aanwijzingen zijn (zoals klachten, signalen van binnen of buiten de organisatie en systeemstoringen), dan kunnen gegevens van (de) betrokken gebruiker(s) worden uitgedraaid, bekeken en gebruikt.
   De betreffende gegevens worden bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een gebruiker noodzakelijk is.

4. Indien en voor zover noodzakelijk kunnen derden ingeschakeld worden bij de werkzaamheden t.a.v. onderzoek en controle.

5. Een beheerder kan tijdens werkzaamheden (kopieerslagen, back-up, restore, reparaties) data zien m.b.t. een gebruiker. De beheerder gaat hiermee op passende wijze prudent om.

Artikel 8. Sancties

Bij handelen in strijd met deze regeling, het bedrijfsbelang of de algemeen geldende normen en waarden voor het gebruik van Internet en e-mail, kunnen afhankelijk van de aard en de ernst van de overtreding maatregelen worden getroffen. Voor personeel gaat het eventueel om disciplinaire en arbeidsrechtelijke maatregelen zoals berisping, overplaatsing, schorsing en beëindiging van de arbeidsovereenkomst.
Voor leerlingen zijn maatregelen denkbaar als ontzegging van de toegang tot het netwerk of tot Internet, tijdelijk of permanent, of andere maatregelen zoals schorsing op grond van overtreding van de huis- en orderegels als bedoeld in de WHW en in het Leerlingenstatuut.
Het is het beheer toegestaan om verboden, aanstootgevend materiaal, bij wijze van voorlopige maatregel, direct te blokkeren. In geval van dreigende storing door gebrek aan opslagcapaciteit is het aan het beheer toegestaan om verboden materiaal (zoals ook amusementsdata, computerspelletjes, film, muziek, pornografie e.d.) zonder toestemming van de gebruiker te verwijderen.

Artikel 9. Rechten van werknemers en leerlingen

Op grond van de Wet Bescherming Persoonsgegevens hebben betrokkenen ten aanzien van de verwerking van persoonsgegevens de navolgende rechten:

1. Inzagerecht: betrokkenen hebben het recht de over hem of haar aanwezige data in te zien. Verzoeken om inzage worden binnen vier weken ingewilligd.

2. Kopierecht: betrokkenen hebben het recht van de over hem of haar aanwezige data een kopie te ontvangen binnen vier weken.

3. Correctierecht: betrokkenen hebben het recht om feitelijk onjuiste gegevens uit de aanwezige data te (laten) verbeteren of aan te vullen. Over verzoeken van correctie of aanvulling wordt binnen vier weken beslist. Indien een verzoek tot correctie of aanvulling wordt ingewilligd wordt de correctie terstond uitgevoerd.

4. Verwijderingsrecht: betrokkenen hebben het recht om de over de hem of haar aanwezige data, die niet (langer) ter zake doen, of in strijd zijn met dit protocol of een wettelijk voorschrift te laten verwijderen en te laten vernietigen. Over een verzoek om verwijdering en vernietiging wordt binnen vier weken beslist. Indien een dergelijk verzoek wordt ingewilligd, vindt de verwijdering en vernietiging terstond plaats.

Artikel 10. Slotbepaling

1. In alle gevallen waarin deze regeling niet voorziet, beslist het College van Bestuur van IRIS.

2. Op deze overeenkomst is uitsluitend Nederlands Recht van toepassing.

3. Geschillen tussen partijen die uit deze overeenkomst voortvloeien, worden voorgelegd aan de terzake bevoegde instantie.

4. Schade aan IRIS of derden veroorzaakt kan op de desbetreffende gebruiker verhaald worden.

Artikel 11. Inwerkingtreding en citeertitel

Dit protocol is vastgesteld door de IRIS-directie op 16 juni 2005, en treedt in werking met ingang van 1 september 2005. Dit reglement treedt in de plaats van eerdere voorschriften en aanwijzingen en kan worden aangehaald als Protocol computernetwerk, e-mail- en Internetgebruik personeel en leerlingen IRIS.