ICT-reglement voor medewerkers en gasten

Christelijke Hogeschool Windesheim

Inhoudsopgave

ICT-reglement Windesheim voor medewerkers

Het gebruik van internet en ICT-middelen is voor (veel van) de medewerkers noodzakelijk om hun werk goed te kunnen doen. Aan het gebruik hiervan zijn echter risico's verbonden die nopen tot het stellen van gedragsregels. Tegen de achtergrond van deze risico's mag van de medewerkers verantwoord gebruik van internet en ICT worden verwacht.

Met dit reglement stelt de Christelijke Hogeschool Windesheim (hierna: Windesheim) regels omtrent het gebruik van deze bedrijfsmiddelen. Het streven daarbij is een goede balans aan te brengen tussen verantwoord en veilig ICT- en internetgebruik en de privacy van de medewerker.
Het gebruik van social media zoals Facebook, LinkedIn en Twitter wordt steeds belangrijker maar kan ook zijn weerslag hebben op Windesheim. Windesheim ondersteunt de open dialoog, de uitwisseling van ideeën en het delen van kennis van de medewerker met vakgenoten en derden via deze sociale media .Voor een goede balans tussen open dialoog en het Windesheim belang worden hier bepaalde regels aan gesteld.
Windesheim is als werkgever bevoegd regels te stellen omtrent de uitvoering van het werk en de goede gang van zaken op de werkvloer. Dit reglement is behalve op de wet ook gebaseerd op artikel E-1, lid 1 t/m 3, van de cao-hbo.

Op grond van het Medezeggenschapsreglement is dit ICT-reglement ter instemming aan de CMR voorgelegd.

Het ICT-reglement voor medewerkers van Windesheim is gebaseerd op de Model AUP reglementen voor het Hoger Onderwijs, een gezamenlijk product van SURFnet en SURFibo.

Begrippenlijst

Bedrijfsvoering:	de Dienst Bedrijfsvoering die die binnen Windesheim belast is met het als beheerder verzorgen van de toegankelijkheid, configuratie, continuïteit en beveiliging van de ICT-faciliteiten. De bevoegdheid voor uitvoering van de bepalingen in dit reglement is binnen Windesheim belegd bij de directeur Bedrijfsvoering. Operationeel handelen is deels gedelegeerd aan medewerkers van het ICT-bedrijf.
Client apparatuur	alle eindgebruiker apparatuur zoals laptop, desktop, usb apparaten, tablet of mobiele telefoon.
Datalek:	persoonsgegevens die in handen vallen van Derden die geen toegang tot die gegevens (mogen) hebben.
Gast	degene die anders dan op grond van een overeenkomst met instemming van Windesheim gebruik maakt van ICT-faciliteiten van Windesheim.
Gebruiker	de medewerker, student of gast die rechtmatig toegang heeft verkregen tot of rechtmatig gebruik maakt van de ICT-faciliteiten van Windesheim.
ICT-faciliteiten	de door of namens Windesheim ter beschikking gestelde faciliteiten voor elektronische informatie uitwisseling, waaronder intranet, internet, elektronische leeromgeving, e-mail, e-mailadres, telefonie en alle faciliteiten al dan niet met een gebruikersnaam/wachtwoord beschikbaar, evenals (draadloze) aansluitfaciliteiten ten behoeve van mobiele apparatuur. Het betreft hier zowel apparatuur als programmatuur als verbindingen. De omschrijving van ICT-faciliteiten is niet limitatief en kan worden aangevuld met faciliteiten zoals die in de toekomst ter beschikking worden gesteld.

Mailbox	ruimte, ingericht op een opslagmedium van een computer, die exclusief ter beschikking staat van de gebruiker voor ontvangst, opslag en verzending van elektronische post.
Medewerker	degene die op grond van een arbeidsovereenkomst of een andere overeenkomst (bijvoorbeeld uitzendovereenkomst, detacheringsovereenkomst, overeenkomst van opdracht) werkzaamheden verricht voor Windesheim.
Student	een ieder die onderwijs volgt bij Windesheim, met inbegrip van extraneï en cursisten.
Verkeersgegevens	gegevens die informatie geven over het gebruik van de digitale systemen, zoals bandbreedte gebruik en soort netwerkverkeer (http, ftp,..).

Artikel 1 Gebruik van ICT-faciliteiten

1.1 Het reglement stelt regels ten aanzien van het gebruik van de ICT-faciliteiten door medewerkers. Doel van deze regels is de goede orde te bepalen ten aanzien van:
   a. systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;
   b. tegengaan van intimidatie, discriminatie en andere strafbare feiten;
   c. bescherming van privacygevoelige informatie waaronder persoonsgegevens van medewerkers en studenten;
   d. bescherming van vertrouwelijke informatie van Windesheim en zijn medewerkers en van studenten;
   e. bescherming van de intellectuele eigendomsrechten van Windesheim en derden waaronder het respecteren van de licentieafspraken die van toepassing zijn binnen en voor Windesheim;
   f. voorkomen van negatieve publiciteit;
   g. kosten- en capaciteitsbeheersing.

1.2 Beperkt privégebruik van internet en ICT-middelen door de medewerker is toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden of het netwerk van Windesheim.

1.3 Gebruik door de medewerker van ICT-faciliteiten voor nevenwerkzaamheden is niet toegestaan, tenzij de medewerker hiervoor schriftelijke toestemming van Windesheim heeft verkregen.

1.4 Dit reglement geldt voor medewerkers en gasten in de zin van de begrippenlijst van dit reglement. Dit reglement geldt niet voor (gast)studenten; op hen is het ICT-reglement studenten van toepassing.

1.5 Windesheim streeft in het kader van handhaving van dit reglement naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele medewerkers zo veel mogelijk beperken. Indien nodig zal slechts geautomatiseerd gecontroleerd of gefilterd worden zonder dat daarbij inzage wordt gegeven in gedrag van individuele personen.

1.6 Medewerkers hebben ieder hun eigen verantwoordelijkheid ten aanzien van informatiebeveiliging binnen de eigen invloedssfeer. Voor het uitoefenen van hun werkzaamheden hebben zij middelen en bevoegdheden toebedeeld gekregen. Zij zijn daarmee ook verantwoordelijk voor een juist gebruik daarvan.

1.7 Iedere medewerker wordt geacht een datalek of vermoeden daarvan te melden bij de servicedesk (servicedesk@windesheim.nl).

1.8 Medewerkers worden geacht (vermoedens van) misbruik of beveiligingsincidenten direct te melden bij CSIRT (CSIRT@windesheim.nl) of bij het ICT-loket (servicedesk@windesheim.nl; C0.72; tel 9070).

Artikel 2 Intellectueel eigendom en vertrouwelijke informatie

2.1 De medewerker dient vertrouwelijke informatie en privacygevoelige informatie waaronder persoonsgegevens waar hij in het kader van het werk toegang toe heeft, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen.

2.2 De medewerker maakt geen inbreuk op de intellectuele eigendomsrechten van Windesheim en derden en respecteert de licentie-afspraken zoals die van toepassing zijn binnen en voor Windesheim.

2.3 De zeggenschap over de informatie van Windesheim berust bij Windesheim. De medewerker heeft geen zelfstandige zeggenschap over de informatie behalve als deze hem expliciet is toegekend door Windesheim. Alvorens beschadigde of defecte privé apparatuur door de medewerker ter reparatie of afvoer wordt aangeboden, dienen alle op het apparaat aanwezige Windesheim data gewist te worden.

2.4 Het is de medewerker niet toegestaan om grote hoeveelheden artikelen uit de bestanden van de digitale bibliotheek te downloaden of substantiële delen van de bestanden of databases in de digitale bibliotheek systematisch te kopiëren.

2.5 De medewerker besteedt bijzondere aandacht aan het treffen van maatregelen zoals in artikel 2.1. genoemd, indien in het kader van het uitvoeren van de werkzaamheden de verwerking van vertrouwelijke informatie buiten Windesheim noodzakelijk is zoals via E-mail, in niet instellingsgebonden Cloud-toepassingen, op externe opslagmedia of eigen client apparatuur. Indien Windesheim met betrekking tot het waarborgen van de vertrouwelijkheid voorschriften heeft vastgesteld zal de medewerker deze naleven.

2.6 De bepalingen uit dit artikel gelden in het bijzonder voor systeembeheerders, voor wie schending van deze bepalingen als een zeer ernstig plichtsverzuim wordt aangemerkt gezien hun bijzondere positie.

Artikel 3 Gebruik van ICT-faciliteiten

3.1 ICT-faciliteiten worden aan de medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie. Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.

3.2 De medewerker 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 worden gedeeld. Bij een vermoeden van misbruik van een wachtwoord kan het systeembeheer per direct het betrokken account ontoegankelijk maken.

3.3 Windesheim kan voor onderwijs- en andere bedrijfsdoeleinden systemen of applicaties voorschrijven. Indien dit van toepassing is zal de medewerker voor de betreffende functionaliteit alleen deze systemen gebruiken en de daarbij gestelde beperkingen en eisen stipt naleven.

3.4 Het aansluiten van servers en actieve netwerkcomponenten (zoals access points en routers) is niet toegestaan zonder toestemming van de directeur Bedrijfsvoering.

3.5 De medewerker mag zelf software op client apparatuur installeren mits deze software legaal verkregen is. Bij problemen met client apparatuur draagt Bedrijfsvoering echter alleen zorg voor het herinstalleren van software die daar oorspronkelijk door Bedrijfsvoering op geplaatst is.

3.6 Het aansluiten van eigen client apparatuur (zoals laptops, tablets en telefoons) is alleen toegestaan op de daarvoor beschikbaar gestelde (wireless) netwerkaansluitingen. De directeur Bedrijfsvoering kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit reglement, zoals een verplichting tot het installeren van virusscanners en wachtwoordbeveiliging.

3.7 Het loskoppelen van ICT-apparatuur die niet voor mobiel gebruik bedoeld is, is de medewerker niet toegestaan.

Artikel 4 Gebruik van e-mail en andere ICT-communicatiemiddelen

4.1 Het e-mailsysteem en de bijbehorende mailbox en e-mailadres worden aan de medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie.

4.2 Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.

4.3 Verboden bij elk gebruik (privé of niet) van ICT-communicatiemiddelen is echter in ieder geval:

a. het verzenden van berichten met een pornografische, racistische, discriminerende, bedreigende, beledigende of aanstootgevende inhoud;
b. het verzenden van berichten met een (seksueel) intimiderende inhoud;
c. het verzenden van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld of enig ander strafbaar feit;
d. het versturen van spam (ongewenste berichten aan grote groepen gebruikers tegelijk), kettingbrieven of kwaadaardige software zoals virussen, Trojaanse paarden of spyware.

4.4 In geval van ziekte, onverwacht langdurige afwezigheid of grove nalatigheid van de medewerker ten aanzien van de uitoefening van zijn functie is Windesheim gerechtigd een vervanger of leidinggevende toegang tot de bestanden of mailbox van de medewerker te verschaffen, doch uitsluitend als dit een zwaarwegende reden van bedrijfsbelang tot toegang oplevert en indien aangetoond kan worden dat het onmogelijk is de toestemming van de medewerker te verkrijgen. Een aanvraag tot toegang moet schriftelijk of per e-mail bij de ServiceDesk ICT ingediend worden door de directeur waaronder de medewerker valt. De directeur Bedrijfsvoering beslist in deze. De vervanger of leidinggevende mag zich echter geen toegang verschaffen tot als privé gemarkeerde mappen, als privé herkenbare mails, of tot mails verzonden naar dan wel afkomstig van een vertrouwenspersoon, bedrijfsarts, bedrijfsmaatschappelijk werker en/of adviseur P&O.

4.5 E-mailberichten van leden van het medezeggenschapsorgaan onderling, van bedrijfsartsen, van bedrijfsmaatschappelijk werkers en van een ieder die zich op grond van de wet op vertrouwelijkheid mag beroepen, worden niet gecontroleerd. Dit geldt niet voor geautomatiseerde controle die noodzakelijk is om de veiligheid van het e-mailverkeer en netwerk te garanderen.

Artikel 5 Gebruik van internet

5.1 De toegang tot internet en bijbehorende faciliteiten worden aan de medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie.

5.2 Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.

5.3 Het is de medewerker niet toegestaan programmatuur te gebruiken die het functioneren van het netwerk en de overige computerfaciliteiten in gevaar kan brengen. In geval de effecten van programmatuur op het netwerk bij de medewerker niet bekend zijn, dient hij deze programmatuur eerst door medewerkers Bedrijfsvoering te laten testen.

5.4 Verboden bij elk gebruik (privé of niet) van internet en bijbehorende faciliteiten is in ieder geval:

a. sites te bezoeken die pornografisch, racistisch, discriminerend, bedreigend, beledigend en/of aanstootgevend materiaal bevatten;
b. filesharing- of streamingdiensten (zoals internetradio of internetvideo) te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de faciliteiten in gevaar kan brengen;
c. films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de medewerker daadwerkelijk weet of had behoren te weten dat dit in strijd is met auteursrechten of andere rechten van intellectueel eigendom;

d. films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.

Artikel 6 Gebruik van sociale media

6.1 Windesheim ondersteunt de open dialoog, de uitwisseling van ideeën en het delen van kennis van de medewerker met vakgenoten en derden via de sociale media. Indien het gebruik van sociale media werkgerelateerde onderwerpen betreft, dient de medewerker ervoor te zorgen dat het profiel en de inhoud in overeenstemming zijn met hoe hij zich in tekst, beeld en geluid zou presenteren ten overstaan van collega's en studenten. In alle gevallen blijft het de plicht van de medewerker om zich fatsoenlijk en als goed medewerker te gedragen.

6.2 Wanneer de medewerker een sociale-media-account opzet dat direct werkgerelateerd is maar op naam van de medewerker is gesteld, zullen de medewerker en Windesheim bij beëindiging van het dienstverband c.q. de arbeidsrelatie tijdig een passende oplossing zoeken voor het overdragen van dit profiel of de informatie en contacten daarop.

Artikel 7 Monitoring en controle

7.1 Controle van gebruik van de ICT-faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit dit reglement voor de doelen genoemd in artikel 1.1. Verboden gebruik van de ICT-faciliteiten kan langs technische weg onmogelijk gemaakt worden.

7.2 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 ter zake verantwoordelijken beschikbaar gesteld. De directeur Bedrijfsvoering kan tot nadere technische maatregelen besluiten.

7.3 Bij vermoedens van overtreding van de regels kan controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het e-mail- en internetgebruik van de medewerker. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.

7.4 Windesheim houdt zich bij het controleren op het niveau van (individuele) verkeersgegevens of persoonsgegevens onverkort aan de Wet bescherming persoonsgegevens en andere relevante wet- en regelgeving. In het bijzonder beveiligt Windesheim de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang daartoe contractueel verplicht tot de vereiste en noodzakelijke geheimhouding.

7.5 Voor client apparatuur die op welke wijze dan ook synchroniseert met de Windesheimomgeving geldt dat alle informatie en alle berichten (dus ook privé) die gemaakt, opgeslagen, ontvangen of verstuurd worden en meegaan in de synchronisatie beschouwd worden als Windesheimdata en als zodanig zijn deze data aan dezelfde controlemaatregelen onderhevig als alle andere Windesheimdata.

7.6 Enkele specifieke maatregelen die Windesheim ter controle kan uitvoeren, zijn:

a. controle ter voorkoming van negatieve publiciteit en intimidatie; de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van filtering van de inhoud op trefwoorden.

b. controle in het kader van kosten- en capaciteitsbeheersing; deze wordt beperkt tot het op basis van verkeersgegevens nagaan van de bronnen van kosten of capaciteitsvraag (zoals de adressen van internetradio en internetvideosites). Als deze websites tot grote kosten of overlast leiden, worden zij geblokkeerd of wordt de beschikbare bandbreedte voor de verbinding naar deze websites beperkt, zonder daarbij de vertrouwelijkheid van de inhoud van de communicatie te schenden;

c. controle op het gebruik van beeldmateriaal; deze vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.

Artikel 8 Procedure bij gericht onderzoek

8.1 Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens betreffende een specifieke medewerker worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit reglement door die medewerker.

8.2 Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de directeur van de betreffende Dienst of het betreffende Domein of van de directeur Bedrijfsvoering. Het College van Bestuur ontvangt een afschrift van deze opdracht en een vastlegging van de resultaten van het onderzoek. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.

8.3 In afwijking van de vorige leden vindt gericht onderzoek naar de beveiliging of integriteit van randapparatuur plaats door systeembeheerders naar aanleiding van concrete aanwijzingen;opdracht van een directeur is daarvoor niet nodig. De resultaten van dit onderzoek worden alleen gedeeld met de medewerker met het doel de beveiliging of integriteit van de randapparatuur te verbeteren. Bij herhaalde constatering van het onveilig zijn van de randapparatuur van een medewerker zal de procedure genoemd in het tweede lid worden gevolgd.

8.4 Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de faciliteiten. Als gericht onderzoek nader bewijs oplevert voor het vermoeden van overtreding van dit reglement, kan Windesheim overgaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Dit vereist voorafgaande schriftelijke toestemming van het College van Bestuur, waarbij de redenen worden genoemd op grond waarvan deze wordt verleend. Windesheim zal zich maximaal inspannen de identiteit van de personen die deze kennisneming uitvoeren, geheim te houden. De vastlegging van de resultaten van het kennisnemen wordt onder naam van de directeur Bedrijfsvoering gedaan.

8.5 Enkele specifieke persoonsgebonden maatregelen die Windesheim ter controle kan uitvoeren, zijn:

a. controle op het uitlekken van vertrouwelijke informatie vindt plaats op basis van steekproefsgewijze controle op trefwoorden. Verdachte berichten worden apart gezet voor nader onderzoek in overleg met het College van Bestuur en/of een directeur;
b. controle op overtreding van het in artikel 4.3 bepaalde vindt plaats door twee personen naar aanleiding van een klacht of op basis van steekproef e-mailberichten te laten openen en de inhoud te laten raadplegen. Deze personen zijn gebonden aan de vereiste en noodzakelijke geheimhouding over de specifieke inhoud.

8.6 De medewerker wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur van het eigen Domein of de eigen Dienst over de aanleiding, de uitvoering en het resultaat van het onderzoek. De medewerker wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou schaden.

8.7 Systeembeheerders verschaffen zich slechts toegang tot accounts of computers van medewerkers als de medewerker daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan in dringende gevallen (bijvoorbeeld wanneer andere gebruikers schade berokkend kan worden) of bij een duidelijk vermoeden van schending van dit reglement, zoals nader bepaald in dit artikel. De medewerker zal in dat geval achteraf worden geïnformeerd.

8.8 Ten behoeve van beheerwerkzaamheden kan het noodzakelijk zijn dat technisch beheer toegang heeft tot accounts van medewerkers. Alle beheerders zijn gehouden aan “de integriteitscode voor ICT beheerders” en zullen niet inhoudelijk kennis nemen van de data en eventuele bestanden die zich op zo’n account bevinden.

Artikel 9 Rechten van de medewerker

9.1 Persoonsgegevens die in het kader van dit reglement verwerkt worden, worden overeenkomstig de Wet Bescherming Persoonsgegevens behandeld[1].

9.2 Tegen besluiten op grond van dit reglement kan door de medewerker binnen zes weken na bekendmaking van het besluit een bezwaarschrift worden ingediend. Daarbij is de Bezwarenregeling Personeel Christelijke Hogeschool Windesheim van toepassing.

Artikel 10 Consequenties van overtreding

10.1 Het handelen in strijd met dit reglement kan worden aangemerkt als het niet handelen als goed medewerker. De in hoofdstuk P van de CAO voor het Hoger Beroepsonderwijs genoemde disciplinaire maatregelen kunnen van toepassing zijn.

10.2 Indien de directeur Bedrijfsvoering kennis neemt van onwettig gebruik van de ICT-faciliteiten door een gebruiker kan hij, onverminderd de sanctiemogelijkheid als bedoeld in dit artikel, aangifte doen bij de politie.

10.3 Disciplinaire maatregelen kunnen niet worden getroffen uitsluitend op basis van een langs geautomatiseerde wijze uitgevoerde verwerking van persoonsgegevens, zoals een constatering door een automatisch filter of blokkade. Voorts worden geen disciplinaire maatregelen getroffen zonder dat de medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

10.4 In afwijking van het voorgaande is het mogelijk dat Windesheim bij (geautomatiseerde) constatering van overlast een tijdelijke blokkade van de betreffende faciliteit invoert. Deze blokkade zal zolang worden gehandhaafd tot aangetoond is dat de oorzaak is weggenomen. Bij herhaling van de oorzaak kunnen zo nodig disciplinaire maatregelen worden genomen.

Artikel 11 Slotbepaling

11.1 Dit reglement is op 12 december 2017 door het College van Bestuur vastgesteld en treedt voor onbepaalde tijd in werking op 1 januari 2018. Dit ICT-reglement voor medewerkers en gasten treedt in de plaats van het reglement zoals vastgesteld bij besluit 718 op 16 december 2014.

11.2 Aan nieuwe medewerkers wordt dit reglement bij aanvang van hun werkzaamheden bekend gemaakt.

11.3 In gevallen waarin dit reglement niet voorziet en een voorziening noodzakelijk is, beslist het College van Bestuur.

11.4 Dit reglement kan worden aangehaald als “ICT-reglement medewerkers”.

[1] Zie https://infosite.windesheim.nl/Pages/Bescherming-Persoonsgegevens.aspx?filterLetter=P