Håndbog i behandling af personoplysninger. PIXI-version

Gefion Gymnasium

Gefionhåndbogen, 2024-2025

GEFION GYMNASIUM

Gymnasiefællesskabet

Indledning

I denne håndbog kan du læse de regler for behandling af personoplysninger, der gælder for alle medarbejderne på Gefion Gymnasium (kapitel 1).

Dette er "pixi-versionen" af Håndbog i behandling af personoplysninger. Den uredigerede udgave (samt denne pixi-udgave) kan findes på Gefion Gymnasiums hjemmeside samt på drev ("alle-lærere" -> "GDPR").

Kapitel 1 - Retningslinjer for behandling af personoplysninger der gælder for alle medarbejderne på Gefion Gymnasium

Gefion Gymnasiums leveregler for datasikkerhed (alle)
En nem måde at komme i gang med at udøve persondatabeskytte og informationssikkerhed på i det daglige er ved at vænne sig til at efterleve følgende enkle leveregler i praksis:

1. Brug **passwords** (eller fingeraftryk som adgangskode) på din computer, smartphone mv. og opdater med et nyt, unikt password hver gang systemet beder om det (hvilket på computeren er hver 6. måned) – eller oftere. Memorér passwords og undlad derved så vidt muligt at skrive det ned. Et password må under ingen omstændigheder fremgå af noter, der er tilgængelige for andre. Tast aldrig passwords mens computeren er koblet til projektor eller lignende, hvor passwordet kan aflures.

2. Log ud eller luk computeren, hvis du forlader den (fx i klasselokalet)

3. Vær varsom med **fysiske dokumenter** med personoplysninger. Læg dem i aflåst skab, skuffe eller kontor - og altid før, du forlader skolens lokaler

4. Papirdokumenter med personoplysninger skal altid bortskaffes ved **makulering (kontakt kontoret) eller i den indrettede papircontainer (aflåst)**

5. **E-mails** med fortrolige og følsomme personoplysninger sendes fortrinsvis via E-Boks, med krypteret mail eller Sikker Mail (Rmail). Mails fra xxx@gefion-gym.dk er TLS krypteret og godkendt i arbejdssammenhæng

6. Hvis personoplysningerne er modtaget eller sendt via **e-mail**, slettes mailen senest 1 måned efter sagsbehandlingen/relevansen af informationen er afsluttet/aktuel

7. Bidrag til løbende at **slette** sager og oplysninger, herunder personoplysninger, der ikke længere er relevante. En mail vil sjældent være relevant, når den er mere end et par måneder gammel

8. Undlad at gemme personoplysninger på USB-nøgle, på skrivebordet på din bærbare computer eller lignende (usikre) **steder**

9. Tag ikke nye it-systemer eller digitale platforme i brug, uden at det er godkendt af ledelsen (AML). I forhold til digitale platforme gælder ovennævnte, hvis det er obligatorisk, at eleven bruger den i undervisningen

10. Udvis **fortrolighed** om de personoplysninger, du bliver bekendt med som led i dine arbejdsopgaver – del og videregiv ikke personoplysninger uden at være sikker på, at det er i orden

11. Åben ikke mails der ser mistænkelige ud eller som kommer fra afsendere, du ikke kender

12. Ved **tyveri eller bortkomst af it-udstyr** (fx pc, tablet og/eller smartphone, som man har fået udleveret som arbejdsredskab på Gefion Gymnasium), skal man straks kontakte AML (alternativt BHB) og MFO

13. Kontakt nærmeste leder eller IT-administrator, hvis du bliver opmærksom på noget mistænkeligt

14. Din computer er dit arbejdsredskab som kun må bruges til arbejdsrelaterede opgaver

Handlepligt i tilfælde hvor der kan være sket brud på datasikkerheden (bl.a. læk)

Hvis der opstår en situation, hvor der kan være sket et brud på datasikkerheden for personoplysninger skal man STRAKS kontakte uddannelsesleder Andreas Lange (AML) og IT-ansvarlig Mikkel Fog (MFO) som hjælper med håndteringen.

Årsagen til at man skal reagere straks er, at Gefion Gymnasium har pligt til at håndtere et sikkerhedsbrud straks og en eventuel anmeldelse til Datatilsynet skal ske uden unødig forsinkelse inden 72 timer, og derfor er det nødvendigt at komme i gang meget hurtigt.

Følgende er eksempler på brud på datasikkerheden:

	Hændelse
1	Man har trykket på et link i sin arbejdsmail, som viser sig at indeholde en virus, der straks spreder sig til hele skolens it-netværk og filer. Dette kan resultere i, at al skolens data, herunder CPR-numre, helbredsoplysninger mv. om skolens medarbejdere bliver krypteret og låst. Skolen har backup af sine systemer, men det er også lykkes bagmændene at kryptere noget af back up'en.
2	Man får stjålet eller mister sin arbejdscomputer (bærbar eller stationær). På computeren findes der fx: • MUS- eller mødereferater med personoplysninger • Økonomiske oplysninger, fx betalingskortoplysninger • Sager om it-support med skærmprint eller kopier af personoplysninger fra it-systemet • Systemadgange uden stærke passwords Alle Gefions arbejdscomputere er krypterede, men vi vil gerne vide det straks, hvis den bliver stjålet/bortkommet
3	Man sender (pr. post eller e-mail) personoplysninger til en forkert modtager

Når bruddet er konstateret og AML/MFO og DPO er inddraget, får vi i fællesskab overblik over skaden.

DPO'en vurderer, om hændelsen er et sikkerhedsbrud, der skal anmeldes til Datatilsynet og om der evt. også skal ske underretning af de berørte registrerede personer.

Instruks om adfærd til forebyggelse og håndtering af hackerangreb

Hvis uheldet er ude, og din computer, smartphone mv. rammes af hackerangreb, skal du **STRAKS**:

- Trække computerens netværksstik ud af væggen (hvis det er en stationær computer)
- Slukke udstyret
- Kontakte Mikkel Fog (MFO) og nærmeste leder. Disse kontakter DPO'en

Du skal ikke betale den løsesum, som hackerne evt. kræver. Årsagen er, at du ikke kan være sikker på at få den fulde kontrol over computeren og filerne tilbage, selvom du betaler.

Medarbejderadfærd til forebyggelse af hackerangreb på Gefions it-udstyr og skolens it-systemer:

1. Du skal holde din computer (og evt. også bærbar computer, smartphone, tablet, mv.) **ajour med de seneste versioner af software og antivirus**, da det giver den bedste sikkerhed. Det er især programmer som Java, Adobe Reader og Flash Player, du selv skal sørge for opdatering af. Microsoft-programmerne opdateres automatisk af Gefion Gymnasium

2. Skolen sørger for daglig **back up** af alt materiale på netværksdrevet og i de systemer, som skolen har godkendt til persondata

3. Vær **skeptisk overfor e-mails**, som er mistænkelige i sprog, layout eller den sammenhæng, du modtager dem i. Det gælder også, selvom mailen umiddelbart kommer fra en kendt afsender. Spørg din nærmeste leder eller it-administrator, hvis du er det mindste i tvivl

4. Vær især **forsigtig med at åbne links eller vedhæftninger**, hvis mailen er mistænkelig, jf. pkt. 3.

5. Hvis du er nødt til at åbne en vedhæftet fil eller link, *selvom* mailen er mistænkelig, kan du begrænse skaden ved at **åbne filen eller linket via din smartphone i stedet for på computeren**. Årsagen er, at smartphonen ikke har adgang til netværksdrevet

6. Hvis du er i tvivl om, hvordan instruksen skal efterleves i praksis, kan du kontakte it-administrator

7. Du skal holde dig ajour med vores awareness-program; *Vipre*. Vipre sender dig engang imellem små video-kurser, som du skal gennemføre

Disse it-systemer må du bruge som medarbejder ("Positivliste"):

Som ansat på Gefion Gymnasium skal du bruge de it-systemer, som skolen stiller til rådighed, til al arbejdsrelateret, digital kommunikation og opbevaring. Dette er især vigtigt, når du behandler **personoplysninger**.

De it-systemer, som Gefion Gymnasium har godkendt til **personoplysninger**, er følgende systemer (**se særskilt om, *hvad Lectio samt cloud-tjenester som fx Google og apps må bruges til længere nede i dette dokument***):

Til alle medarbejdere:

- Outlook (mail)
- Office365
- HRdatabasen
- Gymbetaling

Til administrative medarbejdere og studievejledere:

- Outlook (mail)
- Office365

- E-Boks
- Lectio
- Optagelse.dk
- Netprøver.dk
- Bibliotekssystemet Boss
- DocuNote ESDH
- Statens lønsystem og LDV
- Navision stat
- Indfak2
- HRdatabasen
- Gymbetaling
- CPR-Registeret

Hvis der opbevares (følsomme) personoplysninger i Google, skal de enten slettes eller overføres til et godkendt it-system (fx DocuNote) hurtigst muligt – dog senest 1 måned efter endt brug eller, når de ikke længere har relevans for arbejdet. Undgå som udgangspunkt at gemme følsomme oplysninger i drev.

1 Mailpolitik

Ansatte på Gefion Gymnasium skal bruge de systemer, som skolen stiller til rådighed til al arbejdsrelateret kommunikation. De vigtigste regler er følgende:

1. Arbejdsrelaterede mails sendes fra og modtages i Gmail

2. Mails med fortrolige og følsomme personoplysninger skal som udgangspunkt altid sendes til e-Boks eller med krypteret mail. Mails fra Gefions Gmail- adresser er som udgangspunkt altid krypteret (TLS), og kan derfor også bruges til ovenstående internt, men man skal være meget opmærksom på at slette oplysninger, som man ikke længere skal bruge (senest 1 mdr. efter). Se nedenfor for yderligere kryptering (Rmail)

3. Der må ikke bruges andre mailkonti end medarbejderens officielle skolemail til skolerelateret indhold. Derfor må der aldrig laves videresendelsesregler, eller videresendes til andre mailkonti (fx hotmail og lignende)

Straks efter en medarbejders fratræden lukkes medarbejderens mailadresse ned.

Medarbejderen skal selv være opmærksom på, at mails med følgende typer af personoplysninger max må opbevares i 1 måned efter, sagen/relevansen for arbejdsopgaven er slut: fortrolige og følsomme personoplysninger (dvs. oplysninger om trivsel, studievejledning, psykolog, diagnoser, ordblindhed, fraværsårsager, sociale problemer, gæld, kriminalitet, familiestridigheder og lignende). Når der er gået mere end 1 måned fra den sag, som mailen angik er slut og/eller relevansen for arbejdet ikke længere kan konstateres, skal mailen enten slettes eller overføres til et sikkert it-system (DocuNote), hvis den skal gemmes.

Arbejdsrelaterede e-mails er skolens ejendom, som skolen kan åbne og læse i særlige tilfælde. Dette sker dog kun, hvis det er strengt nødvendigt af hensyn til driften eller som led i fx it-support, som du evt. selv anmoder om. Dvs. at vi ikke foretager fx stikprøvekontroller af indhold i mails mv. [1]

Vi læser ikke medarbejderes e-mails der er tydeligt mærket ”privat”. Du skal bruge privat mailkonto til private beskeder.

Du må heller ikke bruge din arbejdsmail til logins på apps og tjenester (fx Netflix o.lign.).

Private mailkonti må ikke bruges til arbejdsrelateret kommunikation.

<u>Kryptering af mails</u>

Alle mails afsendt via skolens Gmail er som udgangspunkt krypteret (med TLS). Krypteringen sker, når mailen forlader IT-Center Fyns server, og dekrypteringen sker, når mailen når frem til modtagerens

[1] Hjemlen til Gefion Gymnasiums adgang til medarbejdernes mailkonti findes i GDPR art. 6 litra e.

mailboks. Medarbejderen skal ikke selv foretage sig noget i krypterings- og dekrypteringsfasen. Kontoret, studievejledere og ledelsen vil have en ekstra mulighed for at sætte et ekstra krypteringslag på deres mails (Rmail). Hvis man som medarbejder vurderer, at man har et ekstraordinært behov for en ekstra krypteringsmulighed ved afsendelse af mail så kontakt administrationen.

Hvordan sendes der besked til e-boks

Administrationen, ledelsen og studievejlederne har mulighed for at sende post til elever eller forældres e-boks via DocuNote.

Brugeradgange og rettigheder

Medarbejderne på Gefion Gymnasium må kun behandle personoplysninger i de systemer, som Gefion Gymnasium har godkendt til formålet.

Den enkelte medarbejder på Gefion Gymnasium gives personlige autorisationer og rettigheder til systemerne. Adgangskoder til systemerne må derfor ikke deles med andre og må kun "huskes" af systemet, hvis der er tale om en personlig computer.

Overflødiggjorte autorisationer lukkes. Har man som medarbejder en autorisation, som ikke længere svarer til, hvad man har behov for til udførelsen af sine arbejdsopgaver, men som derimod giver adgang til flere personoplysninger eller flere IT-systemer end nødvendigt, skal man straks give sin nærmeste leder besked herom. Det vil sige, at man som medarbejder selv skal reagere og kontakte sin nærmeste leder, hvis man har adgang til "for meget" eller "for lidt", eller hvis man er i tvivl om, om dette er tilfældet.

Sletning af mails

For at sikre at mails med personoplysninger ikke opbevares for længe, skal hver medarbejdere én gang månedligt gennemgå sin mailkonto (indbakke inkl. undermapper, sendt og slettet post).

2 Dette må du bruge Lectio til

Lectio kan bruges til (lærere):

- Elevers fraværsregistrering
- Skema, mødeindkaldelser o.lign.
- Aflevering af skoleopgaver
- CPR-numre og karakterer, da vi pt. ikke har et alternativt opbevaringssted

Gefion Gymnasium bruger ikke Lectios kommunikationsfunktioner (fritekstfelter), da disse funktioner ikke er sikre nok til at fx oplysninger om elevers sygdom, trivsel og sociale forhold kan registreres der. Gefion bruger i stedet **e-mail** til at kommunikere om den slags.

I Lectios kommunikationsfunktioner (fritekstfelter) skriver vi kun helt kortfattede, ikke-fortrolige personrelaterede oplysninger, fx "møde afholdt", "fravær drøftet", mv.

I studievejledningen og administrationen bruges DocuNote (ESDH) og de i heri oprettede elevmapper til studievejledning, sanktionssager, lægeerklæringer, SU- og SPS-ansøgninger. Her har ledelsen, administrationen og studievejlederne adgang.

På skolens hjemmeside under fanen "sikker kommunikation med Gefion Gymnasium" kan elever, værger og medarbejdere se, at vi opfordrer til kun at kommunikere om helt få ting via Lectio, herunder at det kun er de prædefinerede fraværsmuligheder ("Andet", "Kom for sent", Skolerelaterede aktiviteter", "Private forhold", "Sygdom"), der må bruges. Eleverne og forældre opfordres til ikke at uddybe fraværet i fritekstfeltet.

<u>Fortrolighed omkring oplysninger i Lectio</u>

Det understreges, at man naturligvis ikke må bruge sin Lectio-adgang til at se oplysninger, som man ikke har en tjenstlig årsag til at kende.

Via Lectios systemlog kontroller administrator, at data i Lectio kun bruges til tjenstlige formål og ikke uvedkommende formål. Administrator gennemgår standardmæssigt loggen 1 gang halvårligt og efter behov ved konkret mistanke om uhensigtsmæssig brug af Lectio.

<u>Hvem står for oprydningen i de oplysninger, der allerede ér registreret</u>

Ledelsen og administrationen står for at få slettet de gamle oplysninger om afgåede elever (og fx studievejleder- og administrativ note for nuværende elever) i Lectio.

Skolens Lectio-administrator sørger for sletning af afgåede elever og fratrådte medarbejderes adgang til Lectio via modulet "Datasletning"

<u>Hvad må fælles undervisningsnetværksdrev som Google bruges til?</u>

På Gefion Gymnasium benytter vi os af Google igennem EduLife. Edulife-tjenesten leveres af Wizkids.

For Google gælder der på Gefion Gymnasium (med henvisning til de beskrevne retningslinjer for behandling af personoplysninger i denne håndbogs kapitel 1):

- Personoplysninger må kun behandles af ansatte som er beskæftigede med de opgaver som er formålet med den givne behandling/opbevaring. Personoplysninger må ikke ukritisk lægges ud på Drev.
- Man skal som altid behandle personoplysninger med omhu. Google (gennem WizKids) garanterer, at deres system (GSuite såvel som GMail) er sikkert, så der i teorien gerne må ligge følsomt data. Men vi anbefaler, at man ikke lægger følsomt data på drev. Der må heller ikke behandles ellers opbevares personfølsomme eller fortrolige oplysninger i cloud-tjenester/skyer som fx Dropbox. Dropbox må kun bruges til almindelige data som ikke er personhenførbare hverken direkte eller indirekte (gælder både almindelige og følsomme oplysninger).

3 Password-politik

Når man modtager sit password fra Gefion Gymnasium, er det meget vigtigt, at man straks ændrer det til et nyt, personligt, komplekst password.

Det nye password skal indeholde følgende:

- Mindst 8 karakter (men flere – jo længere, jo stærkere)
- Blandede store og små bogstaver
- Tal
- Specialtegn

Passwordet skal skiftes når systemet beder om det, men det må gerne skiftes oftere.

Passwordet skal skiftes, hvis kollegaer eller andre kan have set eller lånt det.

Passwords må kun "huskes" af systemet, hvis der er tale om en personlig computer med unikt login fra forsiden.

Memorér dit password og undlad at skrive det ned. Et password må under ingen omstændigheder fremgå af fx poste it's, der sidder på computeren.

Tast aldrig dit password mens din computer er koblet til en storskærm eller lignende, hvor passwordet kan aflures

Sletning af udtjente digitale arbejdsredskaber

Det sker løbende, at man som medarbejder får nye digitale arbejdsredskaber (fx pc, MAC, tablet, smartphone eller lignende). Udtjente digitale arbejdsredskaber skal i den forbindelse afleveres til IT, der sørger for effektiv og korrekt sletning af arbejdsrelateret data. Har man mulighed at købe det udtjente arbejdsredskab til privat eje, og ønsker man dette, skal udstyret inden købet forbi IT for en tilsvarende effektiv sletning af arbejdsrelateret data.

Om brugen af Apps i undervisningen

Man skal være opmærksom på, hvilke apps man bruger i undervisningen, om app'en er obligatorisk for eleven – og om det kræves at eleven logger ind (fx via Unilogin eller ved at oprette en konto, hvor der skal afgives personoplysninger). Der er IKKE tale om apps hentet fra udbydere som vi allerede har

databehandleraftaler med (fx Google Apps, App Store, Google Play, Chrome webshop) men udelukkende om apps der er afgrænset fra ovenstående, og som modsvarer følgende kriterier:

· Eleverne er tvunget til at bruge dem i undervisningen

· Eleverne skal logge ind med deres Unilogin/personlige oplysninger for at få adgang (her skelnes igen mellem apps i undervisningen og undersøgelser igangsat fra skolens side som fx elevtrivselsundersøgelsen, hvor skolen laver en individuel databehandleraftale med udbyderen). Det kunne være visse quizapps (ikke Kahoot), apps om klima og vejr og/eller Youtube, hvis det kræves, at eleven har en konto og logger ind (altså ikke kun streamer noget).

Handling: Bruger man en app, som modsvarer dette, så skal man handle. Man kan man komme om det på én af følgende måde:

Lad i stedet for brugen være frivillig for eleverne og stil evt. et alternativ til rådighed. Ifølge reglerne skal man også gerne have taget stilling til, om virksomheden bag app'en har udarbejdet en privatlivspolitik, og at der i app'en sker mulighed for indhentelse af nødvendige samtykker til at bruge den (det gør stort set alle firmaer etc. nu om dage) og i den forbindelse, at det er muligt at trække samtykket tilbage og få slettet sine oplysninger i app'en.

Man skal sikre sig at der kan laves en databehandleraftale med skolen inden brugen.

Det kan være svært at lave en statisk liste over apps der bruges i undervisningen, da man jo bruger lidt forskelligt nogle gange – og fremover også vil det. Er man i tvivl om ovenstående i forhold til om den obligatoriske app man bruger i undervisningen kunne være noget, som man skal handle på, så kontakt uddannelsesleder Andreas Lange eller Gefion Gymnasiums DPO, Anne Schultz (ansc@itcfyn.dk).

Generel IT- sikkerhed – hvad kan du selv gøre? Hurtig tjekliste

- Fortæl aldrig dit password til andre. Hvis du mener at nogle kender dit password, så skal du ændre det til et nyt. Brug ikke et password på skolen som du bruger privat (fx til Facebook el. lign.).
- Pas på med at bruge fremmede USB- nøgler. De kan indeholde virus, malware og lignende. Bed hellere om at få tilsendt filer på e-mail
- Brug ikke USB-nøgler som sikkerhedsbackup
- Husk at låse din skærm, når du går fra din PC.
- Lad være med at svare eller åbne e-mails med ukendt eller mistænkeligt indhold og afsender
- Behandl skolens data forsvarligt, og forhold dig kritisk til de netsteder, du besøger
- Lad være med at installere ukendte programmer på din PC
- Lån ikke din PC ud til andre
- Bruger du Smartphone ifb. med arbejdet, skal den sikres med adgangskode, pinkode el. lign.
- Det anbefales, at medarbejdere der arbejder med personfølsomt materiale (adm. personale, studievejledere o.lign.) ikke tager fysiske kopier indeholdende følsomme personoplysninger med hjem. Hvis det alligevel sker, skal man være opmærksom på, at uvedkommende ikke har adgang til oplysningerne. Det anbefales, at de fysiske kopier (med personfølsomme oplysninger) tages med tilbage til skolen og/eller makuleres, når der ikke længere er behov for at have dem liggende i fysisk form. Almindelig opgaveretning o.lign., som underviserne foretager, kan uden problemer tages med hjem i fysisk form.

4. Instruks om beskyttelse af persondata udenfor Gefion Gymnasiums lokaler (hjemmearbejdsplads)

Når man arbejder med personoplysninger udenfor Gefion Gymnasiums lokaler (fx på hjemmearbejdsplads) er sikkerheden særligt udfordret både fysisk og teknisk. Fx er risikoen for tyveri øget. Dette kræver særlig omtanke.

Sikkerhedskravene til arbejde med personoplysninger uden for skolens lokaler er:

1. Hvis personoplysninger midlertidigt (undtagelsesvist) opbevares på en bærbar pc, i Google, på USB-nøgle eller i papirform, skal personoplysningerne overføres til et godkendt it-system på Gefion Gymnasium hurtigst muligt og allersenest 1 måned efter sagsbehandlingen er afsluttet. Samtidig slettes personoplysningerne fra det usikre opbevaringssted.

2. Medarbejderen skal sørge for, at familiemedlemmer og andre uvedkommende ikke får adgang til personoplysninger som led i hjemmearbejde.

3. Den bærbare computer, tablet eller smartphone samt tilhørende passwords er medarbejderens personlige arbejdsredskab og må ikke deles med eller udlånes til andre – heller ikke familiemedlemmer

4. Man skal gå på nettet via VPN, da dette er skolens sikre netværk

5. Instruks om sletning af datamedier ifbm. privat køb af udtjente arbejdsredskaber

Det sker, at man som medarbejder på Gefion Gymnasium får et nyt digitalt arbejdsredskab (pc, mac, tablet, smartphone eller lignende), og at man samtidig får tilbudt at købe det udtjente arbejdsredskab af Gefion Gymnasium til privat eje.

Inden det udtjente arbejdsredskab overgår til medarbejderens privat eje, **skal** det forbi IT-administratoren, som gennemfører en effektiv sletning af arbejdsrelaterede data, herunder personoplysninger, på det udtjente redskab.

Det er kun IT-administratoren, der kan gøre dette, da der kræves særlige programmer. Sletning med de standardfunktioner, som er til rådighed på det udtjente redskab, giver ikke tilstrækkelig sikkerhed for, at sletning er effektiv og uigenkaldelig.

Som led i køb af det udtjente arbejdsredskab modtager man faktura. Heri kvitterer man for, at det udtjente redskab har været til sletning hos IT-administratoren.