IT- og datapolitik

Formål med denne sikkerhedspolitik er at definere rammerne for styring af informationssikkerhed på Fjerritslev Gymnasium

Gyldighed

Sikkerhedspolitikken gælder for alle ansatte, al anvendelse og al adgang til gymnasiets interne informationssystemer i henhold til skolens *Persondatahåndbog* samt Persondataforordningen (GDPR) og gældende dansk lovgivning.

Behandlingssikkerhed

Fjerritslev Gymnasium anvender en risikobaseret tilgang, hvor beskyttelsesniveauet og omkostningerne hertil er baseret på konsekvensanalyser, som foretages årligt.

Denne it-sikkerhedshåndbog gennemgår løbende vedligeholdelse, og indeholder beskrivelser af implementerede tiltag ift. informationssikkerhed samt henvisninger til relevante politikker, retningslinjer og procedurer beskrevet i skolens *Persondatahåndbog*.

Organisation og ansvar:

Bestyrelsen har det ultimative ansvar for informationssikkerheden.

Rektor er ansvarlig for styringsprincipperne og delegerer specifikke ansvarsområder for beskyttelsesforanstaltninger, herunder anvendelse af informationssystemer.

IT-afdelingen rådgiver, koordinerer, kontrollerer og rapporterer om status på sikkerheden ud fra understøttende retningslinjer og procedurer som angivet i nærværende dokument.

Den enkelte medarbejder er ansvarlig for at overholde sikkerhedspolitikken og er informeret herom i denne *IT- og datapolitik* samt skolens *Persondatahåndbog*.

Dispensationer

Dispensationer til gymnasiets informationssikkerhedspolitik og retningslinjer kan i sjældne tilfælde forekomme og skal godkendes af IT-afdelingen ud fra retningslinjer udstukket af ledelsen.

Rapportering

IT-afdelingen og medarbejdere skal informere ledelsen ved mistanke om muligt sikkerhedsbrud uden unødig forsinkelse (ref. skolens *Persondatahåndbog)*.

Gymnasiet fører en samlet oversigt over alle forekomne datasikkerhedsbrud, og IT-afdelingen fører status over dispensationer i en årlig rapport til skolens ledelse.

Ledelsen behandler årligt gymnasiets sikkerhedsstatus og aflægger rapport til bestyrelsen.

Forsætlig overtrædelse og misbrug af reglerne i dette dokument rapporteres af IT-afdelingen til gymnasiets ledelse og skolens DPO uden unødig forsinkelse.

Dispensationer til IT-og datapolitikkerne

Der kan forekomme enkelte situationer, hvor det er nødvendigt at dispensere for de fastlagte politikker. I sådanne tilfælde skal gymnasiets ledelse underrettes, og dispensationen skal gives skriftligt og tidsbegrænset.

Omfatter dispensationen behandling af følsomme personoplysninger skal dette ledsages af en risikoanalyse og tilladelse skal indhentes fra gymnasiets ledelse med information til skolens DPO før dispensationen gives.

Den skriftlige dokumentation af en disposition skal således som minimum indeholde følgende oplysninger:

- Hvilke data er berørt af dispenseringen
- Hvem berør dispensationen
- Konsekvens af dispenseringen (risikovurdering)
- Hvor længe kan dispensation tillades

Opbevaring af personlige oplysninger

Fysisk opbevaring (ref. PDH afsnit 9)

Gymnasiet opbevarer underskrevne samtykkeerklæringer fra elever og ansatte i administrationens elektroniske arkivmapper. Samtykkeerklæringer fra ansatte scannes til de individuelle mapper og for elever lægges samtykkeerklæringerne normalt i en fælles mappe for årgangen.

Deltagerlister fra personalets IT- og datasikkerhedskurser scannes og gemmes i en mappe der er oprettet til formålet i det elektroniske personalearkiv.

Skolens krypterede administrationsserver befinder sig fysisk hos EUC Nordvest, Thisted.

På kontoret opbevares:

Regnskabsmateriale for indeværende regnskabsår og sidste regnskabsår (kassebilag, fakturaer – kan indeholde personfølsomme oplysninger på elever (SPS) og ansatte)

Løndata for indeværende og sidste regnskabsår inkl. diverse refusionsanmodninger syge/fleks/barsel - censoroplysninger med karakterer for eksterne elever.

Sygefraværssedler

"bus"-mappe med køreskiver for chauffører, erfaringserklæringer (cpr.nr.)

Personalemapper for alle ansatte (aktive) medarbejdere i kalenderåret:

Kopi af ansættelseskontrakter, Eksamens- og kursusbeviser, personalesager, skriftlige advarsler, høringer og høringssvar mv.

SPS-data for elever indtil 5 år kalenderår efter det år hvori de dimitterer eller afbryder deres uddannelse (cpr.nr., ansøgninger, bevillinger, fakturaer, anmodninger).

SU-data (ansøgninger)

Arkivskabe i kælder og pengeskabe på adm.gangen

Arkivskabe i kælderen er særskilt aflåste og nøgle hertil opbevares i pengeskab på vicerektors kontor hvortil følgende har adgang (kode):

Sekretærer Peter Niemann Pedersen og Mattias Bodilsen

Vicerektor Anders Kristian Krogh

Pengeskabene på adm.gangen er aflåste. Nøglerne opbeaveres i nøgleskab på kontoret.

I arkivskabene i kælderen opbevares følgende:

Personalemapper for alle fratrådte medarbejdere indeholdende:

- Kopier af ansættelseskontrakter
- Eksamens- og kursusbeviser
- Personalesager i op til 5 år efter fratrædelsen
- Afskedigelse/opsigelser i op til 20 år efter fratrædelsen

I elevmapperne opbevares eksamensprotokoller, kopier af eksamensbeviser i 30 år.

Kopi af eksamensbeviser fra adgangsgivende skoler, standpunktskarakterer opbevares i 5 år.

Regnskabsmateriale opbevares for forrige år og foregående tre år

Brug af elektronisk dokumenthåndtering

Skolens elektroniske arkiv er en filserver hvor der oprettes en mappe til hver elev og ansat på skolen. Dokumenter tilføjes enten ved simpel filflytning eller ved indscanning.

Alle sekretærer og ledere har adgang til disse mapper.

Slettefrister

Slettefrister af de registreredes personlige oplysninger er angivet i gymnasiets *Persondatahåndbog* afsnit 5.

Overholdelse af disse tidsfrister sikres ved følgende procedurer:

Hvert år i uge 43 gennemgås samtlige fysiske og elektroniske arkivmapper mhp. sletning / makulering af forældede oplysninger.

Skulle personlige oplysninger ved en fejl blive videregivet til uberettigede modtagere, tages straks kontakt til den uberettigede modtager som bliver bedt om at returnere eller slette disse data straks og at kvittere når det er foretaget.

Adgang til skolen og aflåste områder

(ref. PDH afsnit 9)

Adgang til gymnasiet

Skolen er åben får direkte adgang på hverdage i tidsrummet kl. 7 til 16:30. Uden for denne tid er skolens bygninger udstyret med alarm. Følgende personer har nøgle/nøglebrik til skolens bygninger udenfor normal åbningstid:

Alle medarbejdere har alarm-kode og nøglebrik til hoveddøren samt nøgle til klasselokaler, lærerværelse osv.

Pedeller, rengøringspersonale, kontorpersonale og ledelse har endvidere nøgle til administrationen.

Udvalgte elever har nøglebrik til specifikke områder, fx fællesområde, musiklokaler og idrætsfaciliteter.

Følgende personer kan til- og frakoble alarmen til skolens bygninger:

Pedeller kan frakoble alarmen. Øvrigt personale kan frakoble alarmen i en periode på 2 timer, når de opholder sig på skolen efter lukketid (hoveddørene er låst).

Skolens administration

Normal åbningstid for skolens administration (kontor) er hverdage mellem kl. 7:30 og 14:00. Uden for dette tidsrum skal det være aflåst og alarmen slået til med mindre der er personale til stede på kontoret.

Følgende personer har nøgler og kendskab til alarmens koder til administrationen:

Rengøringspersonale, pedel, kontorpersonale, ledelse.

Arkivskabe med personfølsomme oplysninger aflåses hver gang kontoret er ubemandet.

Serverrum

Skolens serverrum er adgangssikret med nøgle. Følgende personer har adgang til rummet: IT-vejleder Janus Roed Ramlov, pedeller, ledelse.

Pengeskab

Skolens pengeskabe befinder sig på administrationsgangen, og følgende personer har adgang: Ledelse. kontorpersonale og pedeller.

Sikring af computerudstyr

Udleveret elektronisk udstyr med mulighed for at lagre data er registreret af den IT-ansvarlige med serienummer på udstyret og – hvis muligt – serienummer på det faste lager (harddisk/SSD).

Computere er udstyret med antivirus program og skal sikres med sikker adgangskode, som brugeren (medarbejderen) vejledes i at oprette ved udlevering af computeren. Harddisken er krypteret og internet browsere er forudindstillet til ikke at gemme brugernavne og adgangskoder.

Brugeren kvitterer for modtagelse og accepterer samtidig ovenstående procedurer ved udlevering af udstyret med dato og underskrift.

I tilfælde af, at udstyret fejler, skal det returneres til skolens IT-afdeling. Brugeren må ikke selv søge at udbedre fejlen og må ikke gøre indgreb i udstyret, f.eks. for at opgradere ram eller harddisk.

Ved mistanke om misbrug af udstyret skal brugeren uden unødig forsinkelse kontakte gymnasiets ledelse eller den IT-ansvarlige.

Returnering af udstyr

Når udstyret ikke længere skal benyttes af medarbejderen skal det afleveres tilbage til IT-afdelingen. Kan udstyret benyttes igen skal harddiskens data slettes med et dedikeret program til sikker sletning.

OBS: Det er ikke tilladt kun at formatere harddisken, da data derved kan gendannes.

Skal udstyret bortskaffes skal harddisk fjernes fra enheden og destrueres særskilt i et omfang, der ikke gør den anvendelig igen.

Backup rutiner

Der foretages backup af skolens server-drev, og der foretages afprøvning af tilfældigt udvalgte data i sikkerhedskopien med faste intervaller.

Gymnasiets administrative program – Lectio

Adgang til personlige oplysninger

I gymnasiets *Persondatahåndbog (PDH) afsnit 6* findes en oversigt over de personalegrupper, der kan tilgå de forskellige personlige oplysninger, både almindelige og følsomme, i programmet.

Nedenstående personalegrupper vil med faste intervaller blive bedt om at angive ny adgangskode:

Personalegruppe:	Adgangsniveau:	Skift af kode:
Studievejledere	Studievejleder	Hver 3. måned
Uddannelsesledere	Fuld adgang	Hver 3. måned
Administrativt personale	Fuld adgang	Hver 3. måned
Rektor / vicerektor	Fuld adgang	Hver 3. måned

Føring af log over afviste adgangsforsøg i Lectio

Der skal føres kontrol med afviste adgangsforsøg til Lectio i form af en log, der angiver dato og tidspunkt for hændelsen, antal forsøg og – hvis muligt – hvem der har forsøgt at skaffe sig adgang uden held.

Denne logning skal sikre hurtig og effektiv reaktion på eventuelle brud på persondatasikkerheden.

Ved afvist adgangsforsøg skal den IT-ansvarlige uden unødig forsinkelse foretage en risikovurdering ud fra de tilgængelige data ved logningen og rapportere log og risikovurdering til gymnasiets ledelse ved passende lejlighed.

Databehandlere

Tillægget *Databehandleraftaler* til *Persondatahåndbogen* indeholder aftaler med alle godkendte databehandlere. Det er ikke tilladt at benytte andre databehandlere uden først at indhente databehandleraftale. Beslutning herom træffes af skolens ledelse i samarbejde med skolens DPO.

Godkendte cloudløsninger

Da arkivering af data i cloudløsninger også er omfattet af persondataforordningen, skal databehandleraftale også forefindes for disse.

For overskuelighedens skyld findes herunder en oversigt over de godkendte udbydere af cloudløsninger. Benytter medarbejderne andre løsninger, må de ikke gemme personlige oplysninger fra skolens registrerede personer på disse cloudløsninger.

Cloudløsning:	Databehandleraftale af den:
Google Drive	25/5 2018
Dropbox	25/5 2018
Microsoft (Office365 / OneDrive)	25/5 2018

Awareness på datasikkerhed

Som ansat på Fjerritslev Gymnasium skal du bruge de it-systemer, som skolen stiller til rådighed, til al arbejdsrelateret, digital kommunikation. De vigtigste regler er følgende:

1. Arbejdsrelaterede e-mails sendes fra og modtages i SkoleKom.
2. Private mailkonti må ikke bruges til arbejdsrelateret kommunikation. Der må ikke videresendes arbejdsrelaterede mails fra SkoleKom til en privat mailkonto.
3. Emails med personfølsomme oplysninger må IKKE sendes til personer udenfor SkoleKom og Lectio (fx til en email-adresse). Kontakt kontoret hvis der er behov for at sende oplysninger af den type ud af huset.
4. Brug **passwords** (eller fingeraftryk som adgangskode) på din computer, ipad og smartphone og opdater med et nyt, unikt password hver gang systemet beder om det. – eller oftere. Husk dit password og undlad at skrive det ned. Tast aldrig dit password mens din computer er koblet til en storskærm eller lignende, hvor passwordet kan aflures. Et stærkt password er et langt password (gerne 10 tegn eller mere).
5. Aktivér din pauseskærm, hver gang du forlader din computer (WIN+L)
6. Din arbejdscomputer må kun benyttes af dig. Den må ikke lånes ud til andre.

7. 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
8. Efterlad ikke **fysiske dokumenter** med personoplysninger f.eks. karakterer fremme.
9. Papirdokumenter med personoplysninger skal altid bortskaffes ved **makulering.**
10. **Print** der indeholder personoplysninger hentes i printeren straks. Overvej hvad du printer.
11. Personfølsomme oplysninger må ikke gemmes i cloudtjenester som gymnasiet ikke har en databehandleraftale med (se liste).

12. Udvis fortrolighed om de personoplysninger, du bliver bekendt med som led i dine arbejdsopgaver –videregiv ikke personoplysninger uden at være sikker på, at videregivelse må ske.