IT-sikkerhedspolitik for ansatte på Aurehøj Gymnasium

1.0 Indledning

Alle ansatte har ansvar for at bidrage til at beskytte egne arbejdsrelaterede og gymnasiets informationer mod uautoriseret adgang, ændring, ødelæggelse og tyveri. Der skal derfor løbende informeres og undervises i IT-sikkerhed.

Skolen er ansvarlig for korrekt og lovlig anvendelse af IT-systemer og skal til enhver tid kunne redegøre for den software, som er installeret på servere og pc'er[1]. Skolen pådrager sig et strafansvar, hvis der findes software, hvortil der ikke findes gyldig licens, eller hvis pc'en på anden vis anvendes i strid med gældende lovgivning.

Skolens IT-systemer skal anvendes på en sådan måde, at det ikke:

- Påvirker tilgængeligheden til skolens IT-systemer
- Påvirker fortroligheden eller integriteten af skolens informationer
- Er til gene for skolens medarbejdere, samarbejdspartnere eller elever
- Skader skolens omdømme

1.1 Formål

Formålet med reglerne er at sikre, at skolens IT-systemer anvendes på en måde, der sikrer tilgængelighed, integritet og fortrolighed af skolens informationer. Formålet er endvidere at sikre, at IT-systemerne anvendes med omtanke og til løsning af arbejdsopgaver for skolen.

1.2 Gyldighedsområde

Nedenstående regler gælder for alle, der anvender skolens IT-systemer, inklusive mobilt udstyr og pc'er, hvad enten disse benyttes arbejdsmæssigt eller privat, og uanset hvor benyttelsen foregår.

1.3 Overtrædelse

Hvis skolen konstaterer ulovlige installationer eller filer, vil medarbejderen blive orienteret herom, hvorefter de vil blive afinstalleret eller slettet.

Ethvert misbrug af skolens IT-systemer eller overtrædelse af disse regler kan medføre en advarsel eller ændring i ansættelsesforholdet, og det kan i gentagne tilfælde eller i særligt grove tilfælde medføre opsigelse og/eller bortvisning.

2.0 Passwordbeskyttelse

Medarbejderens pc, adgang til læringsplatforme (fx Lectio) og øvrige arbejdsrelaterede programmer og platforme skal altid være beskyttet med et sikkert password.

Den ansatte må ikke logge på med en anden persons identitet eller forsøge at få adgang til andre brugeres data. Det er forbudt at tvinge sig adgang til andre personers eller organisationers computersystemer gennem f.eks. "hacking" eller på anden vis. Den ansatte må ligeledes heller ikke forsøge at skjule sin identitet, bortset fra de tilfælde, hvor det eksplicit er tilladt.

Medarbejderen skal opbevare sine adgangskoder på betryggende vis, og koderne må ikke udleveres til andre. Medarbejderen skal låse/logge af pc'en, når den forlades. Dette gælder også eget IT-udstyr som anvendes i arbejdsøjemed, fx en privat smartphone eller tablet, hvor der er fx installeret arbejdsmail.

Gode adgangskoder er lange og består af tal- og bogstavkombinationer (store/små bogstaver) og indeholder min. 8 tegn.

[1] Når ordet pc nævnes i dette dokument, forstås arbejdscomputere, dvs. også MAC, evt. telefon, tablet etc.

Adgangskoden skal ændres minimum hvert halve år.

Regler for passwordbeskyttelse

- Alle enheder, læringsplatforme og skytjenester - også private, som bruges arbejdsrelateret - skal permanent være beskyttet af et sikkert password
- Lav et password på minimum 8 karakterer bestående af både tal og bogstaver og store og små bogstaver
- Skift dit password hvert halve år
- Efterlad aldrig din pc uden passwordbeskyttelse, og overdrag aldrig dit password til andre

3.0 Brug af pc

Medarbejderen (og kun medarbejderen) må benytte den bærbare arbejds-pc til private formål, så længe det ikke strider mod lovgivningen, nærværende retningslinjer og skolens tarv, renommé og værdier.

3.1 Medarbejdere i det offentlige rum samt på rejse

Medarbejdere skal være bevidste om, at andre kan se og høre, hvad de beskæftiger sig med, når de befinder sig i det offentlige rum, fx på vej til og fra arbejde, på tjenesterejser eller til møder. Medarbejderen må som udgangspunkt ikke logge sig på offentlige wifi (fx på cafeer og i tog), men bør i stedet bruge en 3- eller 4G-forbindelse enten via pc-en eller mobil (internetdeling), hvis det er muligt. På tjenesterejser og til møder, hvor Internet er nødvendig, kan man undtagelsesvis benytte f.eks hoteller og konferencecentres WiFi

3.2 Installation af programmer

Der må ikke installeres ulovlige eller ikke-licenserede programmer på medarbejderens IT-udstyr.

3.3 Sikkerhed og antivirusprogram

Skolen er ansvarlig for installering af antivirusprogram og firewall, men medarbejderen skal løbende tilse, at programmerne er opdateret.

4.0 Brug af andet IT-udstyr

4.1 Mobiltelefon, tablet og andet udstyr

Det er tilladt at benytte sin private mobiltelefon arbejdsrelateret og på skolens netværk. Det er dog et krav, at man anvender sikker adgangskode (jf. pkt. 2.0), hvis den anvendes til skolens IT-systemer (fx Lectio, Office365, GoogleApps m.m.) og/eller giver adgang til personfølsomme data om ansatte/elever.
Benyttes tjenstlige mobiltelefoner til overtakserede tjenester, donation af gaver til indsamlinger, udlandstelefoni, mobildatanetværk i udlandet mv., betales det af medarbejderen selv, og der afregnes direkte med økonomiafdelingen. Roaming skal som udgangspunkt være slået fra på udlandsrejser. Undtagelser fra dette aftales på forhånd med ledelsen.

4.2 Anvendelse af Lectio-app på mobile enheder

Det er ikke tilladt at anvende en app til Lectio på en smartphone eller tablet. Lectio indeholder personfølsomme data, og det er vanskeligt at sikre sig, at trafikken mellem Lectio og enheden er tilstrækkelig sikker. Eneste tilladte adgang til Lectio fra mobile enheder er gennem Lectios hjemmeside, evt. gennem en genvej på enheden.

5.0 Lagring af data og backup

Private data må lagres på medarbejderens IT-udstyr i det omfang, materialet er lovligt og ikke skader eller optager plads, så udstyrets ydeevne forringes.

5.1 Håndtering af personfølsomme data

Ansatte på Aurehøj Gymnasium skal overholde Persondataloven og sikre sig, at personfølsomme data (fx vedr. elever, kolleger mv.) opbevares på forsvarlig vis.
Hvis man mister et medie (pc, tablet, telefon, ekstern harddisk el. lign.), som indeholder data, der er personfølsomme eller personhenførbare, skal skolens øverste ledelse orienteres omgående. Datatilsyn og politi vil herefter blive kontaktet om nødvendigt.

5.2 Backup af egen data

Medarbejderen er forpligtet til at tage backup af arbejdsrelateret data, så arbejdet hurtigt kan genoptages ved fx computernedbrud, tyveri, virusangreb osv.

1. **Backup i skyen:** Medarbejderen skal tage backup af arbejdsrelateret data i skytjenesten OneDrive eller GoogleDrive, som stilles gratis til rådighed af skolen som en del af Office365/Google. Det anbefales, at man gør det til en vane at gemme alt arbejdsrelateret data i OneDrive/GoogleDrive og opretter en permanent synkronisering mellem skytjenesten og pc'en.

6.0 Brug af internet

6.1 Besøg på hjemmesider

Privat brug af internettet må finde sted i det omfang, det er foreneligt med medarbejderens varetagelse af sit daglige arbejde på skolen og i øvrigt ikke strider mod lovgivningen, disse regler og skolens værdier.
Det er ikke tilladt at foretage private indkøb eller tilmelde sig private nyhedsbreve, hvor medarbejderens e-mailadresse til arbejdsbrug anvendes som kontaktadresse, da dette kan indikere, at det er skolen, som foretager indkøbet.
Det skal understreges, at medarbejdere ikke må anvende IT-udstyr ejet af skolen eller skolens netværk til bevidst at opsøge hjemmesider med ulovligt indhold.

6.2 Download af musik, billeder m.v.

Downloadet materiale må udelukkende anvendes i overensstemmelse med ophavsretsloven eller anden lovgivning.

6.3 Brug af chat og sociale netværkstjenester

Det er et krav, at medarbejdere, der anvender sociale netværkstjenester, omhyggeligt læser og overholder betingelserne for anvendelse. Det er endvidere et krav, at medarbejderne overholder love og bestemmelser, eksempelvis om copyright og bagvaskelse (injurier).
Det er tilladt at identificere sig som værende ansat på Aurehøj Gymnasium, når medarbejderen repræsenterer skolen loyalt og professionelt, og hvis medarbejderen i forbindelse med tilkendegivelser på personlige blogs eller andetsteds angiver, at indholdet er udtryk for vedkommendes personlige holdning. I øvrigt har ansatte på Aurehøj Gymnasium ret til at ytre sig på lige fod med øvrige offentligt ansatte.

7.0 Brug af e-mail

Adgangen til at anvende e-mail er etableret til skolemæssig brug. Medarbejderens e-mail initialer@aurehoej.dk, er den der primært skal benyttes til korrespondance ud fra Aurehøj. Den anden e-mail aurehoej-gym.dk, er din konto til GoogleApps og bør ikke benyttes til korrespondance med modtagere udenfor Aurehøj. Enhver e-mail sendt via skolens IT-systemer betragtes som skreven korrespondance, der tilhører skolen, og som skolen derfor kan gøre sig bekendt med og disponere over som anden

korrespondance til og fra skolen. Adgang til en medarbejders e-mail på grund af begrundet mistanke om misbrug eller efter anmodning fra myndighederne må kun finde sted efter instruks fra og med godkendelse fra den øverste ledelse. Efterfølgende orientereres tillidsrepræsentanten. Adgangen er begrænset til, hvad der er nødvendigt i forhold til årsagen, og adgangen ophører, når undersøgelsen er afsluttet (se desuden pkt. 8).
E-mails er juridisk bindende på samme måde som andre former for korrespondance, og skal derfor behandles med samme omhu.
Medarbejderen skal udvise særlig agtpågivenhed ved modtagelse af e-mails med potentielt skadelige filer eller links. Som udgangspunkt må man ikke åbne filer eller links fra ukendte afsendere.

7.1 Privat brug af e-mail

Medarbejderens e-mailadresse (initialer@aurehoej.dk) må kun benyttes i arbejdsmæssig sammenhæng.

Dette betyder, at:

- alle medarbejdere opfordres til at oprette en e-mailkonto hos en privat udbyder og bruge denne til private korrespondancer

7.2 Sikker mail

Når en medarbejder på Aurehøj Gymnasium sender eller modtager e-mails med personoplysninger af fortrolig og/eller følsom karakter, skal det jf. persondataloven ske via en sikker mailforbindelse. Det kan være mailkorrespondance i forbindelse med elevoptag, sanktioner, eksamensafholdelse, fravær, frafald, personalesager, indberetninger til UVM, udveksling af oplysninger med andre skoler mv. Kravet om en sikker mailforbindelse opstår, når mailen indeholder fortrolige og følsomme personoplysninger, fx oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold samt oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold. En mailpostkasse er kun sikker, hvis den benytter en sikker krypteringsnøgle. Når vi sender e-mail fra aurehoej.dk benytter vi tvungen kryptering. For at e-mailkorrespondancen bliver sikker, skal både afsender og modtager have en sikker mailpostkasse.

8.0 Lectio

Lectio må bruges til:

1. LMS-system (værktøj til studieplan, lektier, undervisningsbeskrivelser, opgaveaflevering, karaktergivning, bogadministration, fraværsregistrering, almindelig dokumenthåndtering=
2. Skemalægning og eksamensplanlægning
3. Korte beskeder om aflysninger, møder, fravær mv.
4. Følgende må ikke fremgå: Mødereferater, mødenoter, helbredsdiagnoser eller oplysninger, hvoraf man kan udlede en helbredsdiagnose.

Beskedfunktionen i Lectio må ikke anvendes til beskeder *om* elever. Brug i stedet arbejdsmail.

LECTIO MÅ IKKE INDEHOLDE FORTROLIGE ELLER FØLSOMME OPLYSNINGER

CPR-numre og karakterer er fortrolige oplysninger. Disse oplysninger findes i Lectio, som del af studieadministrationen. Derfor er det afgørende, at kun de medarbejdere, der har et tjenstligt formål med at kende personoplysninger om eleverne, fx i form af karakterer eller CPR-numre, bruger deres Lectio-adgang til dette. Underviser man ikke en elev, eller er eleven gået ud, må man derfor fx ikke tilgå elevens oplysninger.
For at beskytte tidligere elevers personoplysninger mod uvedkommendes adgang, er det vigtigt, at man som medarbejder IKKE tilgår oplysninger, selv om det er muligt.
I Lectio er der log tilknyttet adgangen til personoplysninger, som jævnligt kontrolleres af ledelsen.

Det er ledelsen på Aurehøj Gymnasium, der tildeler brugeradgange til Lectio. Vi tilstræber, at man kun får adgang til de oplysninger, som er relevante for at kunne udføre den funktion på Aurehøj Gymnasium, man har som medarbejder.

9.0 Logning, registrering og overvågning

Af hensyn til skolens drifts- og sikkerhedsmæssige forhold og for at sikre, at brugen af skolens IT-systemer foregår i overensstemmelse med skolens politikker, bliver alt, hvad der sker på skolens IT-systemer løbende registreret, ligesom der bliver taget backup af alt, hvad der ligger på systemerne.
De medarbejdere, som har adgang til logfiler og backup, er instrueret i ikke at spore data relateret til enkeltpersoner, selv om det er muligt at gøre dette.
Enhver aktivitet til og fra skolens arbejdspladser kan uddrages og fremlægges i forbindelse med misbrug og/eller retssagsbehandling, hvor skolen er involveret.
Adgang til en medarbejders elektroniske data (e-mail, filer, internetlogfiler m.v.) på grund af mistanke om misbrug eller efter anmodning fra myndighederne må kun finde sted efter instruks fra og med godkendelse fra den øverste ledelse. Efterfølgende orientereres tillidsrepræsentanten. Adgangen er begrænset til, hvad der er nødvendigt i forhold til årsagen, og ophører, når undersøgelsen er afsluttet.
Privat materiale, dvs. materiale, som befinder sig i en mappe/bruger, der hedder ”Privat”/”personlig”, eller mapper/brugere, hvor disse ord indgår i navnet, vil ikke blive omfattet af en eventuel undersøgelse, medmindre der foreligger en dommerkendelse (jf. Straffelovens § 263, stk. 1).
Hvis en medarbejder bliver syg eller i øvrigt uplanlagt er fraværende i længere tid, kan IT-afdelingen hjælpe med at finde materiale frem, hvis det er vigtigt og nødvendigt for skolens drift. En sådan søgning skal ske efter instruks fra øverste ledelse. Medarbejderen og tillidsrepræsentanten skal orienteres om, at en sådan søgning har fundet sted, og søgningen skal ske med tilbørlig hensyntagen til medarbejderens privatlivs fred.
IT-afdelingen kan også aktivere ”ikke til stede-assistenten”. Sådanne handlinger kræver altid godkendelse og tilstedeværelse af den øverste ledelse.

22/09-2021 (KR)
Version 1.2