

PERSONDATA og IT-SIKKERHED



Skanderborg
Gymnasium

Vejledning og retningslinjer om anvendelse og opbevaring af persondata

Revideret januar 2026

INDHOLDSFORTEGNELSE

INDLEDNING.....	5
VIGTIGE BEGREBER	6
PERSONOPLYSNINGER.....	6
<i>Fortrolige og følsomme personoplysninger.....</i>	<i>7</i>
<i>Almindelige personoplysninger</i>	<i>7</i>
OPBEVARING OG BEHANDLING AF PERSONOPLYSNINGER.....	8
HVEM MÅ BEHANDLE PERSONOPLYSNINGER OM ELEVERNE OG OM ANSATTE?	8
HVORDAN MÅ PERSONOPLYSNINGER BEHANDLES OG OPBEVARES?	8
<i>E-mail.....</i>	<i>9</i>
<i>Mobilt udstyr, harddisk (PC eller Mac) og USB-stik.....</i>	<i>9</i>
<i>Personligt netværksdrev (på skolens egne servere).....</i>	<i>9</i>
<i>Internt administrationsnetværksdrev.....</i>	<i>9</i>
<i>Studieadministrativt system (Studica).....</i>	<i>9</i>
<i>Office365.....</i>	<i>9</i>
<i>Andre cloud-systemer, eksempelvis google drev.....</i>	<i>9</i>
<i>MUS.....</i>	<i>10</i>
<i>Slettepolitik</i>	<i>10</i>
DIGITAL SKOLEPOLITIK.....	11
IT-SIKKERHED - HVAD SKAL DEN ANSATTE PÅ SG SELV GØRE?	11
<i>Krav.....</i>	<i>11</i>
<i>Som ansat på SG skal du gøre følgende:.....</i>	<i>11</i>
<i>Retningslinjer</i>	<i>11</i>
PRINCIPPER, REGLER OG RAMMER FOR UNDERVISNINGEN	12
<i>Brugen af ChatGPT i undervisningen</i>	<i>12</i>
SAMTYKKEERKLÆRING TIL ANSATTE PÅ SKANDERBORG GYMNASIUM	13
<i>Offentliggørelse af billeder og videoer</i>	<i>13</i>
<i>Samtykke</i>	<i>13</i>
SAMTYKKEERKLÆRING TIL ELEVER PÅ SKANDERBORG GYMNASIUM.....	13
<i>Retningslinjer</i>	<i>13</i>
<i>Offentliggørelse af billeder.....</i>	<i>14</i>
<i>Behandling af data</i>	<i>14</i>
<i>Elektroniske systemer.....</i>	<i>14</i>
<i>Logning</i>	<i>15</i>

<i>Samtykke</i>	15
HENVENDELSE TIL FORÆLDRE/VÆRGE.....	15
BILAG: CASES	16
CASE 1: MAIL FRA ELEV OM SYGDOM.....	16
CASE 2: KOPIER AF ELEVERS PAS I FORBINDELSE MED STUDIETUR.....	16
CASE 3: BRUG AF KAHOOT I UNDERVISNINGEN	16
CASE 4: LAGRING OG DELING AF KARAKTERLISTER I GOOGLE DREV.....	16
CASE 5: PASSWORD I STUDICA-KERNE/STUDICA-TEAMS.....	17
CASE 6: BRUG AF TEAMS- OG OUTLOOK-APP PÅ TELEFON OG IPAD.....	17
CASE 7: ELEV FORTÆLLER OM SYGDOM	17
CASE 8: ELEV SKAL LAVE EN VIDEOAFLEVERING.....	18
CASE 9: DU OPRETTER EN LUKKET FACEBOOK-GRUPPE TIL DIT HOLD	18
CASE 10: GYMNASIEFEST	18

Indledning

Denne rapport har til formål at afdække anvendelse og opbevaring af personfølsomme data på Skanderborg Gymnasium. Rapporten har desuden til formål at hjælpe ansatte på Skanderborg Gymnasium med at forstå persondatalovgivningen¹ i forbindelse med behandling af personoplysninger på Skanderborg Gymnasium.

Rapporten giver ansatte på Skanderborg Gymnasium et redskab til at kunne arbejde sikkert med persondata. Rapporten giver mulighed for at vurdere, om skolen har behov for at ændre på de rutiner, der anvendes i arbejdet med persondata.

Persondataloven regulerer al behandling af personoplysninger. Behandling er eksempelvis indsamling, registrering, systematisering, opbevaring, søgning, videregivelse eller sletning af personoplysninger, enten elektronisk (Mac, PC, USB-stik, mobiltelefon mv.) eller ikke-elektronisk (fysisk papir med noter, arkiver mv.).

Når der behandles personoplysninger, skal man først gøre sig klart, om man må behandle disse. For at disse personoplysninger må behandles, skal der være et udtrykkeligt angivet og sagligt formål. Oplysningerne skal desuden være relevante og må ikke indeholde mere end hvad der er nødvendigt for formålet. Jo mere følsom en oplysning er, jo mere tungtvejende skal begrundelsen for behandlingen være.

Denne rapport er udarbejdet af uddannelsesleder Jakob Peter Thomsen, IT-medarbejder Anders Elvang og IT-medarbejder Asbjørn Kabel.

¹ Databeskyttelsesforordningen - og de retlige rammer for dansk lovgivning, Betænkning nr. 1565

Vigtige begreber

Personoplysninger er delt i to kategorier, alt efter hvor følsomme de er. Der er (1) almindelige personoplysninger og (2) fortrolige og følsomme oplysninger, som kræver den største forsigtighed.

Personoplysninger

Personoplysninger er enhver form for information om en person (ansat, elev, pårørende mv.) uanset om personen kan identificeres direkte eller indirekte, fx ved hjælp af elevnummer eller andre oplysninger, der er særlige for den pågældende.

Oversigt over personoplysninger

Almindelige personoplysninger	Fortrolige og følsomme personoplysninger
- klassiske stamoplysninger (navn, køn, adresse og telefonnummer, fødselsdato, nær familie, oplysning om status vedr. hemmeligt nummer/adresse) - oplysninger om uddannelse, udtalelser, karakterer, eksamensbeviser, beskæftigelser, deltagelse i hold/fag/grupper/fagniveauer, skriftligt arbejde - almindelige elevklager - oplysninger om opgaveportefølje, løn, skat, pension og lønkontonummer, kørekort - nationalitet - systembrugeroplysninger (uni-login) - oplysninger om fravær, dog ikke begrundelse for fraværet	- personnummer/CPR-nummer - foto-ID - registrering af snyd til eksamen - logning af internetbrug - strafbare forhold - helbredsoplysninger (diagnose og behandling) - væsentlige sociale problemer, interne familieforhold, resultater af personlighedstests, bortvisningsgrund - evt. misbrug af fx alkohol eller stoffer - referater af personlige samtaler, hvis disse indeholder oplysninger af følsom art Oplysninger, der ikke må behandles uden personligt samtykke: - oplysninger om racemæssig eller etnisk baggrund - personlig politisk, religiøs eller filosofisk overbevisning (elevers meninger i undervisningen er ikke at betragte som følsomme oplysninger) - fagforeningsmæssigt tilhørsforhold - seksuel orientering

Fortrolige og følsomme personoplysninger

Behandling af fortrolige og følsomme personoplysninger kræver særlige forholdsregler. Der er forskel på fortrolige og følsomme personoplysninger, hvor de følsomme personoplysninger skal behandles med mere varsomhed end fortrolige personoplysninger. På Skanderborg Gymnasium anvendes sikker mail (kryptering via fx Doc2Mail), hvis der sendes fortrolige og/eller følsomme oplysninger via e-mail.

Det er vigtigt at understrege, at fortrolige og følsomme personoplysninger ikke må gemmes i ikke-sikre cloud-tjenester/skyer som fx google drev eller på ekstern lagringsenhed (USB-stik, ekstern harddisk), som ikke er krypteret med password. CPR-numre er fortrolige personoplysninger. CPR-numre må lægges i skolens Office365 og/eller på medarbejderens arbejdscomputer krypteret med sikkert password. Man bør undgå at lade CPR-numre ligge fysisk fremme uden opsyn i offentligt tilgængeligt rum eller at gemme CPR-numre på digital lagringsenhed uden kryptering med password. Følsomme oplysninger om fx en elevs sygdomsforløb må efter samtykke deles i sikre cloud-tjenester (Teams i Office365) og/eller via sikker mail. Specielt gælder for studievejledere, at de kun må gemme følsomme personoplysninger om elever i Studica eller på det interne administrationsnetværksdrev. Specielt for ledelsen gælder, at de kun må gemme følsomme personoplysninger om medarbejder i et sikkert system. Specielt for administrationen gælder, at de kun må gemme personlige oplysninger om elever i Studica og på internt administrationsnetværksdrev.

Almindelige personoplysninger

Kravene til beskyttelse af almindelige oplysninger er ikke lige så omfattende som kravene til fortrolige og følsomme oplysninger, men de skal benyttes og behandles med omhu og forsigtighed. Det betyder at man skal undgå at offentliggøre almindelige personoplysninger, med mindre man har fået samtykke. Specielt gælder at almindelige personoplysninger som elevens navn, nummer og karakterlister godt må lægges i skolens Office365 og/eller på medarbejderens arbejdscomputer krypteret med sikkert password. Man bør undgå at lade karakterlister ligge fysisk fremme uden opsyn i offentligt tilgængeligt rum eller at gemme karakterlister på digital lagringsenhed uden kryptering med password.

Opbevaring og behandling af personoplysninger

Reglerne i loven omhandler registre med personoplysninger, hvilket vil sige, at alle former for strukturerede samlinger, som er tilgængelige efter bestemte kriterier, er personoplysninger. Det gælder uanset om det er elektronisk eller fysisk.

Hvem må behandle personoplysninger om eleverne og om ansatte?

Ifølge reglerne i sikkerhedsbekendtgørelsen (bek. nr. 528 af 15/06/2000, §11) må kun autoriserede medarbejdere have adgang til givne fortrolige og følsomme persondata. Det er fx kun studievejledere, administration og ledelse, der må have adgang til særligt følsomme personoplysninger om elever, som eleven ikke ønsker delt med fx lærerteam. På samme vis er det kun tilladt for ledelsen at have adgang til fortrolige og følsomme personoplysninger om ansatte. Følsomme personoplysninger om sygdom der har indvirkning på undervisning kan af interessehensyn være nødvendige at fortælle til lærerne. Det kan fx være at en elev skal gennemgå en korsbåndsoperation og derfor vil være fraværende fra undervisningen i en længere periode. I disse tilfælde er læreren at betragte som en autoriseret medarbejder i forhold til sygdomsoplysninger om elever.

Hvordan må personoplysninger behandles og opbevares?

Der er forskellige regler for forskellige personoplysninger og hvilke måder man må transmittere og gemme personoplysninger. Nedenfor uddybes kriterier herfor.

	E-mail	Mobilt udstyr, PC og USB-stik uden kryptering med password	Personligt netværksdrev (på skolens egne servere)	Internt administrationsnetværksdrev	Studieadministrative systemer (Studica)	Office365, herunder Microsoft OneDrive	Andre cloudtjenester
Almindelige personoplysninger	Ja. Slettes efter skolens regler	Ja	Ja	Ja	Ja	Ja	Ja
Personnummer	Ja, skal krypteres	Nej	Ja	Ja	Ja	Ja	Nej
Følsomme og andre fortrolige personoplysninger	Ja, skal krypteres	Nej	Nej	Ja	Ja	Situationsafhængigt	Nej

E-mail

Når der modtages en e-mail, er der ikke sikkerhed for hvem afsenderen reelt er, og man bør derfor ikke åbne eller svare på e-mails med ukendt eller mistænkeligt indhold og afsender. Man bør ikke klikke på ukendte links i en mail. Almindelige personoplysninger må sendes som almindelig e-mail og slettes efterfølgende efter skolens regler; jf. afsnit om sletning. Skal der transmitteres følsomme eller fortrolige personoplysninger over det åbne net, skal e-mailen sendes krypteret.

Mobilt udstyr, harddisk (PC eller Mac) og USB-stik

Der foretages ikke automatisk backup af dokumenter. Såfremt udstyret går i stykker er der risiko for at data går tabt. Almindelige arbejdsdokumenter uden personoplysninger må gerne gemmes på computerens eget drev eller USB, men husk at foretage backup. Du må gerne gemme almindelige og fortrolige personoplysninger på din arbejdscomputer, hvis du har krypteret med password. Det kan fx være navn, adresse, karakterlister og/eller CPR-numre.

Personligt netværksdrev (på skolens egne servere)

Det anbefales, at der løbende foretages backup, således at dokumenter kan genskabes, hvis de går tabt.

Almindelige personoplysninger og CPR-numre må gemmes på det personlige netværksdrev. Følsomme personoplysninger om fx sygdom må ikke gemmes her pga. manglende sikkerhed, bl.a. fordi der ikke foretages logning.

Internt administrationsnetværksdrev

Man må gerne gemme fortrolige og følsomme personoplysninger på skolens interne netværksdrev, som kun er tilgængeligt for administration/studievejledning, og hvor sikringen imod uvedkommende adgang er højere.

Studieadministrativt system (Studica)

Studica anvendes på skolen til at gemme informationer om medarbejdere og elever. Almindelige personoplysninger og CPR-numre må gemmes i det studieadministrative system.

Office365

Almindelige personoplysninger og CPR-numre må opbevares i skolens Microsoft Office365. Følsomme og andre fortrolige personoplysninger må gerne gemmes her afhængigt af interessehensyn. Det kan fx være en besked til et klasseteam om en elevs fravær pga. brækket ben.

Andre cloud-systemer, eksempelvis google drev

Man må ikke gemme fortrolige og følsomme personoplysninger i ikke sikre cloudløsninger som fx google drev.

MUS

Referater af medarbejderudviklingssamtaler betragtes som personfølsomme data. Disse referater føres i Word og gemmes i fildelingsværktøjet OneDrive mellem skolens ledelse.

Slettepolitik

Administration: Tidligere ansatte/elevs adgang til Studica slettes en måned efter ophør af tilknytning til skolen. Ved ophør af et ansættelsesforhold, slettes den tidligere ansattes adgang til Office365 ved overgangen til et nyt skoleår. Ved ophør af ansættelsesforhold slettes den tidligere ansattes personalesag efter fem år med mindre, der foreligger interessehensyn. Det kan fx være i den tidligere ansattes interesse, at man opbevarer en anbefaling i længere tid end fem år.

Pedelkontorets TV-overvågning: Videoer slettes efter 30 dage. Den ledende pedel har adgang til de gemte optagelser indenfor de 30 dage.

Ansatte: Mails med følsomme personoplysninger skal slettes efter 30 dage. De fleste mails indeholder personoplysninger og bør slettes efter maksimum et halvt år. Andre mails kan man have interesse i at bevare i længere tid. Det kan derfor være en god idé at organisere mails i mapper, hvis indhold slettes efter fx henholdsvis 30 dage, et halvt år, et år, tre år og fem år. Du bør desuden sørge for at du jævnligt rydder op i dine filer, således at du fx ikke har fortrolige og personfølsomme oplysninger liggende på dine arbejdsredskaber længere end det er påkrævet.

Som ansat på Skanderborg Gymnasium forventes du at behandle persondata om elever, medarbejdere og andre med relation til Skanderborg Gymnasium i henhold til reglerne beskrevet i denne rapport.

Digital skolepolitik

IT-sikkerhed - hvad skal den ansatte på SG selv gøre?

Skanderborg Gymnasium bestræber sig på at sørge for, at sikkerheden på skolens netværk er høj, og at det samtidig er let at anvende IT i dagligdagen. Alle brugere (elever og medarbejdere) godkendes i vores brugerdatabase, før de får adgang til netværket.

Nedenstående er krav og retningslinjer for den ansattes gøren og laden på SG. Kravene er ufravigelige, mens retningslinjerne skal ses som gode råd til, hvordan man kan øge sin egen og dermed skolens IT-sikkerhed.

Krav

Som ansat på SG *skal* du gøre følgende:

- a) Dine arbejdsrelaterede passwords (herunder også computerpassword) skal være på minimum 10 tegn og indeholde både store og små bogstaver, tal og symboler.
- b) Mac: FileVault skal aktiveres, så harddisken er krypteret.
- c) PC: Windows Defender skal være aktiveret (det er den som standard).
- d) Undlad at gemme fortrolige og følsomme personoplysninger (fx CPR-numre og kopi af pas) på eksterne lagringsenheder (USB-stik, ekstern harddisk), som ikke er krypteret med password.
- e) Ryd jævnligt op i din **arbejds**mailboks (**Outlook**).
- f) Studievejledning og administration: Følsomme personoplysninger (fx sygdomsforløb og referater af personlige samtaler) må kun gemmes på skolens interne administrationsnetværksdrev, OneDrive og Studica.

Retningslinjer

Som ansat på SG *anbefales* følgende:

- a) Fortæl ikke dit password til andre. Hvis andre får adgang til dit password, bør det ændres.
- b) Skift jævnligt dit password og sørg for ikke at lade din Studica-adgang og/eller Teams-adgang være åben uden opsyn.
- c) Ryd jævnligt op i dine filer på din arbejdscomputer.
- d) Vær forsigtig med at bruge fremmede USB-nøgler, da de kan indeholde virus, malware osv.
- e) Undlad at åbne og svare på e-mails med ukendt eller mistænkeligt indhold/afsender.
- f) Forhold dig kritisk til de netsteder, du besøger, og links, du klikker på (også links i e-mails).
- g) Sørg jævnligt for at lave backup af værdifulde data på din PC/Mac. Backup kan med fordel laves i OneDrive, som er en del af skolens office-pakke.
- h) Lad være med at installere ukendte programmer på din PC/Mac.
- i) Vær forsigtig med at låne din PC/Mac ud til andre, da logininformationer kan være lagret herpå.

- j) Vi anbefaler, at almindelige personoplysninger, som fx elevlister med telefonnumre og adresser, kun opbevares på en enhed, der er krypteret med password.
- k) Sørg for, at Outlook, Teams og lignende kommunikationsprogrammer ikke er åbne eller åbner i undervisningssammenhænge, hvor computeren fx er sat til projektor. Undgå at din computer står åben og tilgængelig, når du ikke selv er til stede.

Som ansat på Skanderborg Gymnasium forventes du at behandle persondata om elever, medarbejdere og andre med relation til Skanderborg Gymnasium i henhold til reglerne beskrevet i denne rapport.

Principper, regler og rammer for undervisningen

På Skanderborg Gymnasium har vi fra skoleåret 2024-25 besluttet følgende retningslinjer for brugen af digitale enheder i undervisningen, med fokus på elevernes trivsel, læring, dannelse og fællesskab. Brug af devices er noget, vi som skole skal lære eleverne, da de ikke er digitale indfødte.

1. Devices i skolen er værktøjer til undervisning. Brug af devices i undervisningstiden er således kun tilladt, når det er fagligt relevant.
2. Sociale medier, spil, shopping, streaming og andre former for ikke-undervisningsrelateret underholdning er dermed ikke tilladt i undervisningstiden.
3. I undervisningen kan man med fordel planlægge sekvenser med og sekvenser uden skærm, så elever lærer både faglig brug af devices i undervisningen og også træner offline koncentrationsfastholdelse og anvendelse af analoge læremidler.
4. Mobiltelefoner sættes i flytilstand og placeres i mobilhotellet i klasselokalet ved lektionsstart. Hvis læreren ønsker inddragelse af mobiltelefonerne i undervisningen i faglig sammenhæng, kan de hentes og aktiveres - men altså kun efter lærerønske.
5. Alle computere skal være lukket ved lektionsstart og åbnes først når læreren ønsker det.
6. Internetspærring med firewall er etableret til blokering af udvalgte sider, herunder sider indeholdende de fire S'er (sociale medier, spil, shopping og streaming).

Brugen af ChatGPT i undervisningen

På Skanderborg Gymnasium tillader vi brugen af ChatGPT og lign. kunstig intelligens i undervisningen for både elever og lærere. Det er vigtigt at man som bruger af ChatGPT reflekterer over hvordan man anvender AI. Anvendes det af læreren i undervisningen med eleverne skal de IT-sikkerhedsmæssige rammer for brugen af ChatGPT gøres bevidst for eleverne.

- 1) Undgå at indtaste eller dele personfølsomme oplysninger såsom adresse, telefonnumre, cpr-

numre, karakterhistorik på elever, fraværsoplysninger på elever, SPS/støtteforhold, klager, sanktioner eller lign. i ChatGPT.

- 2) Rapporter eventuelle mistænkelige eller upassende indhold eller adfærd, du oplever, til din lærer eller IT-ansvarlige.
- 3) Brug en stærk adgangskode til og beskyt din adgangskode til ChatGPT.
- 4) Hvis du har mistanke om, at dit login eller adgangskode er blevet kompromitteret, skal du straks skifte adgangskode og underrette din lærer (som elev) eller IT-ansvarlige (som lærer).

Samtykkeerklæring til ansatte på Skanderborg Gymnasium

Offentliggørelse af billeder og videoer

Skanderborg Gymnasium bruger dagligt billeder i både trykte og digitale medier. På den måde er det muligt for elever, forældre, personale, bestyrelse og andre at følge skolens dagligdag. Gennem billeder og film fortæller vi de gode historier, åbner gymnasiet for omverdenen og informerer om begivenheder og arrangementer.

Datatilsynet skelner mellem to typer af billeder: (1) situationsbilleder og (2) portrætbilleder.

Det er tilladt at offentliggøre situationsbilleder uden samtykke. Det drejer sig om billeder, hvor en aktivitet eller en situation er det egentlige formål med billedet, og hvor det ikke er afgørende, hvilke personer der optræder på billedet. Vi har fokus på, at offentliggørelsen skal overholde gældende lovgivning. Ingen skal føle sig udstillet eller krænket. Derfor vurderer vi løbende, hvilke situationsbilleder og videoer der er egnet til at dele med offentligheden, og modtager vi indvendinger, vil et billede eller en video blive fjernet i det omfang, det er muligt.

Et portrætbillede er et billede, hvor personen er det egentlige formål med billedet. Portrætbilleder må ikke offentliggøres uden samtykke.

Samtykke

Som ansat på Skanderborg Gymnasium giver du med din ansættelse automatisk tilladelse til, at Skanderborg Gymnasium må offentliggøre portrætbilleder. Det gælder bl.a. til gymnasiets hjemmeside og andet informationsmateriale, herunder Velkomsthæftet. Hvis du som lærer ønsker, at der er billeder på fx hjemmeside eller officiel Facebook-side der ikke må offentliggøres, skal du aktivt gøre opmærksom på det, ved at henvende dig til administrationen.

Samtykkeerklæring til elever på Skanderborg Gymnasium

Retningslinjer

Skanderborg Gymnasium bruger billeder i både trykte og digitale medier. På den måde er det muligt for elever, forældre, kollegaer og andre interessenter at følge med i skolens dagligdag. Gennem billeder og film fortæller vi de gode historier, åbner gymnasiet for omverdenen, deler viden og informerer om begivenheder og arrangementer. Vi lægger stor vægt på, at offentliggørelsen

overholder gældende lovgivning samt almindelig moral og etik. Ingen skal føle sig udstillet, udnyttet eller krænket. Derfor vurderer vi altid, hvad der er egnet til at dele med andre, og skulle vi modtage indvendinger, vil et billede eller en video blive fjernet i det omfang, det er muligt.

Offentliggørelse af billeder

Datatilsynet skelner mellem to typer af billeder: situationsbilleder og portrætbilleder.

Situationsbilleder kan offentliggøres uden samtykke. Det drejer sig om billeder, hvor en aktivitet eller en situation er det egentlige formål med billedet, og hvor det ikke er afgørende, hvilke personer der optræder på billedet.

Portrætbilleder må ikke offentliggøres uden et klart samtykke fra eleven og forældrene (hvis eleven er under 15 år).

Behandling af data

Som led i din uddannelse på Skanderborg Gymnasium registrerer og behandler skolen personoplysninger om dig. De personoplysninger, vi behandler om dig, er dels de oplysninger, du selv har givet os på dit ansøgningsskema, og dels oplysninger, der stammer fra din skolegang. Vi registrerer således stamoplysninger om dig samt oplysninger om dit skema, dit fremmøde, dit studieforløb, resultater af prøver, års- og eksamenskarakterer samt eventuelle varsler og afgørelser, hvis du har for meget fravær. Personoplysningerne om dig behandles med det formål at dokumentere, at du opfylder betingelserne for at blive indstillet til eksamen på normale vilkår.

Herudover behandles års- og eksamenskarakterer med det formål at dokumentere, at du opfylder betingelserne for at blive student. Nogle af disse oplysninger er vi forpligtede til at videregive til Undervisningsministeriet, Regionen, Styrelsen for Videregående Uddannelser eller dine forældre (hvis du er under 15 år). Skanderborg Gymnasium behandler blandt andet dine persondata i det studieadministrative system, Studica. Personoplysningerne i Studica gemmes på ubestemt tid med henblik på at kunne genskabe et eksamensbevis.

Skanderborg Gymnasium tilbyder studievejledning til vores elever. Som led i blandt andet studievejledningen kan vi komme i berøring med følsomme personoplysninger om dig. Dette sker som hovedregel kun, hvis du giver os oplysningerne, og kun hvis oplysningerne er relevante for din skolegang. Det kan være tilfældet, hvis oplysningerne handler om din trivsel eller dit helbred, for eksempel lægelige oplysninger som led i fravær.

Elektroniske systemer

På skolen anvender vi en række elektroniske systemer, som du selv har adgang til med login og password (Studica, Office365, Netprøver, Unilogin). Disse systemer må kun anvendes til studierelaterede formål. Du må ikke videregive dit login og/eller password til andre. Hvis du ved et uheld kommer til at se andres password, skal du straks give besked til skolens kontor. Anvendelse af andres login og password er ulovligt og kan have alvorlige konsekvenser.

Du har altid ret til at få indsigt i og eventuelt få rettet personoplysninger om dig, som du mener er forkerte eller ufuldstændige, jf. persondatalovens § 35. Endvidere kan du tilbagekalde det samtykke,

du har givet til visse behandlinger, jf. nedenfor. Hvis du ønsker at gøre brug af disse rettigheder, bedes du kontakte skolens kontor.

Logning

Skanderborg Gymnasium udfører logning af alt internet trafik. Logningen foretages for at sikre en etisk forsvarlig brug af internettet i overensstemmelse med skolens IT-regler, og i forbindelse med overvågning af internetbrug under eksamen. Der udføres også logning i Studica, Office365 og Netprøver.

Bemærk at når du er elev på Skanderborg Gymnasium vil skolen i forbindelse med din studieaktivitet:

- behandle og opbevare personoplysninger om stamdata, karakterer, sygdom og fravær i Studica.
- udfører logning af elevers data genereret på Skanderborg Gymnasium for at sikre etisk forsvarlig brug af internettet i overensstemmelse med skolens IT-regler.
- dele elevers UNI-login data med de af skolen godkendte databehandlere, som fx bibliotekssystemet Systematic og Systime.

Samtykke

På Skanderborg Gymnasium indhenter vi samtykke til ovenstående gennem Studica ved din studiestart. I forbindelse med indhentelse af samtykke informeres du om skolens brug af dine persondata.

Henvendelse til forældre/værge

Skanderborg Gymnasium kan have brug for at kontakte dig som forælder/værge til en elev på gymnasiet. Det kan for eksempel være i forbindelse med akut opstået ildebefindende eller sygdom, hvor vi har behov for at kontakte elevens forældre/værger. I tilfælde, hvor det drejer sig om en elevs velbefindende, er det skolens politik at rette henvendelse til forældre/værge uden først at indhente samtykke.

Bilag: Cases

Case 1: Mail fra elev om sygdom

Du modtager en besked fra en elev, hvor eleven beskriver at han ikke har været i skole pga. depression. Hvad gør du med mailen?

Du skal videregive informationen sikkert til studievejlederen og slette beskeden indenfor senest 30 dage. Du videre giver informationen sikkert ved at printe beskeden og give til studievejlederen eller ved at videresende beskeden sikkert. Beskeden sendes fx sikkert ved at sende indenfor skolens interne system (Teams eller fra intern Outlook-adresse til anden intern Outlook-adresse). Du må ikke sende beskeden videre fra en intern Outlook-adresse til en e-mailadresse uden for huset.

Case 2: Kopier af elevers pas i forbindelse med studietur

Du skal på studietur med en klasse og kopierer for en sikkerheds skyld elevernes pas. Må du medbringe fysiske kopier af elevernes pas?

Nej, du må ikke medbringe fysiske kopier af elevernes pas. Hvis kopierne mistes, er der tale om et sikkerhedsbrud. Du skal i stedet scanne kopier og gemme dem på din arbejdscomputer krypteret med password og/eller ekstern lagringsenhed krypteret med password.

Case 3: Brug af Kahoot i undervisningen

Du har lavet en Kahoot med faglige spørgsmål. Du har lavet din Kahoot som en prøve, hvor du ud fra elevernes svar giver eleverne karakterer. Derfor beder du eleverne angive deres fulde navn i Kahoot. Må du det?

Nej, det må du ikke gøre, da oplysning af fuldt navn kræver en databehandleraftale med Kahoot, som vi ikke har. Anbefalingen vil være, at man beder eleverne logge ind i Kahoot med et alias. Et alias må gerne være elevens fornavn, fx Lars P. Logger eleverne ind med deres fulde navn, videregives personoplysninger til en tredjepart, som vi ikke har en databehandleraftale med. Dvs. vi har ikke en aftale med Kahoot, hvor de skriver under på, at de vil behandle data forsvarligt.

Case 4: Lagring og deling af karakterlister i Google Drev

Du deler et hold med en anden lærer og I har delt et google-dokument med en elevliste med navne og karakterer på alle eleverne (karakterliste). Må man det?

Nej, det må du ikke, da det ikke er muligt at lave en databehandleraftale med Google. Dermed er med Google Drev ingen sikkerhed i forhold til, at du deler elevlisten med en tredjepart. Du kan i stedet dele karakterlisten igennem Office365, som vi har en databehandleraftale med.

Case 5: Password i Studica-kerne/Studica-Teams

Du er til undervisning og har logget ind i Studica-kerne/Studica-Teams for at føre fravær. Du logger ikke ud af Studica og lader computeren stå åben. I løbet af timen er du nede for at kopiere et opgaveark til eleverne. Er det et problem at lade Studica stå åbent?

Ja, det er et problem, at eleverne har fri adgang til både din computer og til dit Studica. Eleven vil kunne finde oplysninger på din computer, som kan udgøre et sikkerhedsbrud. Det kan fx være i tilfælde af, at du har en elevliste med CPR-numre liggende på din computer. Det kan også være at eleven går ind i Studica-kerne på din computer for at tjekke karakterer og læser andre eleveres karakternoter, som er at betragte som følsomme personoplysninger.

Case 6: Brug af Teams- og Outlook-app på telefon og iPad

Du har installeret Teams- og Outlook-app på din telefon og på din iPad. Din telefon er sikret med firecifret kode og det er kun dig selv, der anvender din telefon. Din iPad er ligeledes sikret med en firecifret kode, men dine børn låner ofte din iPad til at spille på. Er der problemer med at have installeret Teams- og Outlook som apps på din telefon og iPad?

Der er ingen problemer med at du har installeret Teams og Outlook som apps på din telefon, når du har en firecifret kode og det kun er dig selv, som anvender telefonen. Skulle telefonen blive stjålet er der tale om et sikkerhedsbrud, men hvor der er en tydelig handleplan i forhold til de personoplysninger du evt. har i Teams og Outlook. Her er handleplanen at skifte adgangskode til dit Office365-login. Den samme handleplan vil være gældende, hvis du får stjålet din iPad, hvorpå du har installeret Teams og Outlook som apps. Men det er et problem, hvis du lader dine børn anvende en iPad, hvor du har installeret Teams og Outlook som apps. Hvis dine børn ved en fejl videresender en mail indeholdende følsomme personoplysninger er der tale om et sikkerhedsbrud, som skal meldes til databeskyttelsesrådgiveren. Afhængigt af indholdet i en sådan mail vil man risikere, at datatilsynet skal informeres.

Case 7: Elev fortæller om sygdom

En elev fortæller dig mundtligt, at han ikke har fået lavet sin aflevering, da forældrene er blevet skilt. Eleven fortæller desuden, at han har det svært for tiden, og derfor kan have svært ved at følge med i undervisningen. Må du herefter fortælle resten af Teamet dette?

Nej, det må du ikke uden et samtykke fra eleven. Samtykke kan gives mundtlig eller skriftligt. Dvs. før du informerer resten af teamet skal du spørge eleven, om du må videregive informationen. Får du et samtykke af eleven, skal du informere om, hvem du videregiver informationen til. I dette tilfælde vil man spørge eleven, om man må videregive informationen til klassens lærere.

Case 8: Elev skal lave en videoaflevering

Du har bedt dit hold om at lave en videoaflevering i grupper, hvor kravet er at alle elever optræder i videoen med et fagligt element. Du beder eleverne uploade videoen i youtube og sende dig linket. Må du gøre det?

Her skal du være meget påpasselig. Du må ikke tvinge eleven til at uploade i youtube, da det ikke er muligt at lave en databehandlertaftale med youtube. Eleven kan selv vælge at dele videoen gennem youtube. Sker dette, skal du huske at informere eleverne om at gøre deling af youtube-videoen privat, hvis de ikke ønsker at alle kan se den. Derudover skal du være opmærksom på, at eleven skal anvende deres egens youtube-konto og dermed selv er dataansvarlig for videoen. Hvis skolen har en youtube-konto må videoen ikke uploades her, da skolen så er dataansvarlig for videoen. Det betyder at skolen har ansvaret for, at youtube-videoen ikke bliver delt med tredjepart eller at den skal slettes på foranledning af en elev. Videoafleveringen indeholder følsomme personoplysninger idet eleverne fremgår med billede og lyd af videoen. Deles videoen mod elevens ønske til en tredjepart, er der tale om et sikkerhedsbrud. Ønsker du at øge datasikkerheden kan du bede eleven aflevere i videoen som en mp3- eller mp4-fil, som de sender via Teams eller anden sikker kanal. Du kan også anbefale eleven at anvende Stream som er en del af skolens Office365-løsning.

Case 9: Du opretter en lukket Facebook-gruppe til dit hold

Du opretter som lærer en lukket Facebook-gruppe til dit hold, hvor du kan give og modtage beskeder samt dele undervisningsmateriale. Må du gøre det?

Nej, det må du ikke. Hvis du lægger undervisningsmateriale fra lærebøger ud på en lukket Facebook-gruppe skal du først hente samtykke fra rettighedshaver. Det er rent praktisk en meget omfattende arbejdsproces at skulle gøre dette, hver gang der lægges undervisningsmateriale ud. Du har ingen sikkerhed for, at personer i gruppen ikke deler materiale i den lukkede Facebookgruppe med andre udenfor gruppen ved at linke. Derudover er beskeder til og fra elever følsomme personoplysninger, som ikke må ligge i Facebook. Det kræver at skolen tegner en databehandlertaftale med Facebook, hvilket man principielt ikke kan gøre, da Facebook er opbygget som en individuel app, hvor alle har mulighed for at dele materiale og beskeder. Dvs. du har ingen sikkerhed for, at en personlig besked i en lukket gruppe deles men en person uden for gruppen ved en fejl. Sker dette er der tale om et sikkerhedsbrud.

Case 10: Gymnasiefest

En elev bliver beruset i en sådan grad, at vedkommende kaster op og føler sig dårlig. Må du som lærervagt ringe til elevens forældre for at bede dem hente deres barn?

Ja, det må du gerne. I dette tilfælde drejer det sig om elevens velbefindende. Til gymnasiefester sikrer vi, at vi ikke sender elever ud af huset, hvis vi vurderer, at de vil have svært ved at klare sig selv.