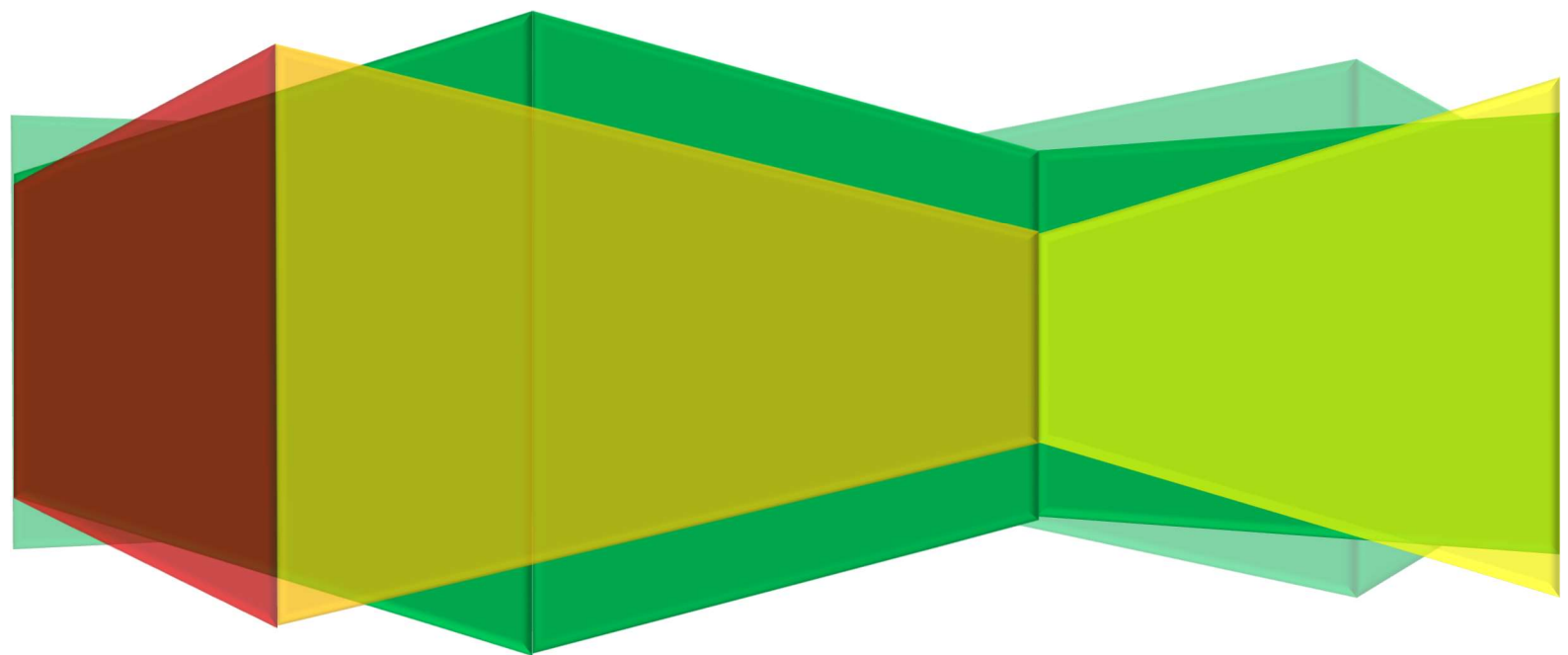


Sorø Privatskole



IT-sikkerhedspolitik



Indhold

IT-sikkerhedspolitik.....	2
Fysisk sikkerhed	2
Datasikkerhed.....	2
Overholdelse af datasikkerhed.....	2
Brugernes ansvar	3
Itslearning	3
Tabulex	3
Hjemmeside.....	3
Infrastruktur	4
Trafik.....	4
Sikkerhedsniveauer	4
Servere.....	4
Andre emner.....	5
Drift.....	5
Pædagogik	7
Formål.....	7
Mål.....	8
Interaktive tavler	8
Indsatser	9
Retningslinjer.....	9
Retningslinjer iPads	10
Sanktioner.....	10
Adfærd.....	11
Eksempler på uacceptabel adfærd.....	11
Vedvarende proces.....	12

IT-sikkerhedspolitik

Det er et lovkrav, at skolen håndterer personfølsomme oplysninger på en forsvarlig måde, da skolen har pligt til at beskytte elever, forældre og medarbejdere jf. Lov om behandling af personoplysninger. Ledelsen, som er den øverst ansvarlige for IT-sikkerheden, skal sørge for, at der til stadighed er etableret procedurer og systemer, der støtter overholdelsen af sikkerhedspolitikken. Sikkerhedsniveauet skal være målbart og kontrollabelt, hvor dette overhovedet er muligt.

Det er skolens ønske at give elever, forældre og medarbejdere gode muligheder for anvendelse af IT uden brug af unødvendige restriktioner, men samtidigt sikre mod misbrug af skolens IT-systemer eller misbrug udført herfra af andre IT-systemer.

Fysisk sikkerhed

Skolen ønsker i videst muligt omfang at sikre de fysiske installationer mod ulykker, hærværk og tyveri. Det sker blandt andet med aflåste døre, alarmsystemer og sikrede rum. Ligeledes sikres i størst mulig omfang mod forsyningssvigt i server rum. Det sker blandt andet i form af ekstra ventilation af server rum på varme sommerdage.

Datasikkerhed

Administrative data repræsenterer en betydelig værdi og skal sikres mod uautoriseret adgang, tab og forvanskning. Ledelsen fastsætter sikkerhedsniveauet for de enkelte systemer, herunder klassificering af data og vurdering af, hvorvidt et egentligt nødberedskab skal etableres. Ledelsen, administrationen og multimedievejlederen står for brugeradministration af elever, forældre og medarbejdere på intranettet og skolens iPads. Ledelsen fastsætter backup-procedurer og viruspolitik, men det er op til den enkelte effektuere det på sin enhed. Det er også ledelsen, der træffer beslutning om eventuel logning, e-mail politik og anvendelse af internet.

Overholdelse af datasikkerhed

Ledelsen vil løbende sikre sig at sikkerhedspolitikken efterleves. Brud på sikkerhedspolitikken rapporteres til skolens ledelse. Brud på sikkerhedsreglerne vil

have konsekvenser for den pågældende bruger og kan i yderste konsekvens medføre bortvisning fra skolen.

Brugernes ansvar

Skolen gemmer kun personfølsomme oplysninger på den sikrede administrations-server, intranettet eller medarbejderens private drev på skolen. Der gemmes ikke personfølsomme oplysninger på flytbare medier såsom filhosting-services på internettet, bærbare enheder, USB-Sticks, CD'er m.m. UNI-login og andre koder er personlige og må ikke udlånes til andre. Brugere bliver automatisk logget af deres enhed, intranettet eller Tabulex, når de er inaktive i et stykke tid.

Itslearning

Itslearning leverer skolens intranet. Itslearning har ikke placeret data i tredjelande, og at Itslearning gør generelt ikke brug af Safe Harbour-ordningen. De persondata, som Itslearning har adgang til, i kraft af deres rolle som databehandler, befinder sig alle i deres hostingcenter i Lyngby. (Specifikt om SkoleIntra og håndtering af personlige oplysninger her <http://www.itslearning.dk/haandtering-af-personlige-oplysninger>)

Tabulex

Tabulex databehandler på vegne af skolen. Tabulex har i de seneste 6 år fået gennemført en RS3000 revision. Revisionen gennemgår Tabulex' procedurer og arbejdsgange overfor sikkerhedsbekendtgørelsens 19 paragraffer (<http://www.tabulex.dk/om-os/revisionserklaering>).

Hjemmeside

Skolens hjemmeside er Hypertext Transfer Protocol Secure (HTTPS), så kun afsender og modtager kender meddelelsen. Det sikrer opskrivningen, og herunder udvekslingen af CPR-numre, på skolens hjemmeside, når forældre anmoder om at blive skrevet på skolens venteliste.

Infrastruktur

Skole, SFO og Klub har adgang til et stabilt og sikkert trådløst netværk med tilstrækkelig kapacitet set ud fra et sikkerheds- og læringsmæssigt perspektiv. Det er vigtigt, at infrastrukturen er velfungerende, så det ikke bliver en barriere, et irritationsmoment eller en sovepude for brugen af digitale læremidler.

Trafik

Langt hovedparten af internettrafikken, der generes på skolen, er fra elever og medarbejdere, og den bliver leveret over WiFi. Den øvrige del af trafikken er næsten al sammen genereret af administrationen. Internettrafikken bliver tilgået fra elevernes og medarbejdernes enheder (iPads, Macs, PCer, smartphones m.m.).

Sikkerhedsniveauer

- Elevernes WiFi-sikkerhed:
Løsning: 802.1x – certifikat løsning, højeste wireless sikkerhed. Al trafik kører i en dobbelt-krypteret IP-Sectunnel fra klient til accesspunkter og til Aruba Controller. Kode: UNI-login, personligt
- Lærernes WiFi-sikkerhed:
Løsning: 802.1x – certifikat løsning, højeste wireless sikkerhed. Al trafik kører i en dobbelt-krypteret IP-Sectunnel fra klient til accesspunkter til Aruba Controller. Kode: UNI-login, personligt
- Administrationen WiFi-sikkerhed:
Løsning: WPA2-PSK med AES incryption. Al trafik kører i en dobbelt-krypteret IP-Sectunnel fra klient til accesspunkter til Aruba controller.

Servere

- Administrations-server-sikkerhed:
Windows 2008R2 serverlicens, netværksopdelt, opdateret efter Microsoft update:
 1. Back-up, remote – opdateres dagligt
 2. PF-Senfe, firewall mod internettet

3. Aruba, firewall mod wifi
4. Fil-server med AD bruger, sikkerhed på fil-share med dagligt backup
- Undervisnings-server-sikkerhed:
Windows 2008R2 serverlicens, opdateret efter Microsoft update:
 1. AD brugere, opdelt i forhold til lærer/elever med rettigheder
 2. PF-Sense, firewall mod internettet
 3. Aruba, firewall mod WiFi

Andre emner

Aruba Clearpass – validering af UNI-login koder mod elever/lærerne på WiFi og styrer Apple-TV.

Drift

Skolen anvender 1:1 fordeling af enheder. Dvs., at samtlige medarbejdere og elever på 1.-6. årgang råder over minimum én enhed (f.eks. en iPad eller bærbar Mac). Eleverne på 7.-9. årgang medbringer deres egen enhed. Det giver en let tilgængelig adgang til de digitale læremidler både i skolen og dagtilbuddene.

I forhold til fælles programmer, apps og abonnementer foretages der fælles indkøb, så ressourcerne udnyttes optimalt og mulighederne for videndeling optimeres. Det skal være klart for den enkelte, hvad der er til rådighed, og det er vigtigt, at de forskellige programmer, apps og abonnementer er til rådighed på alle på skolen og dagtilbuddene.

Skolen anvender et mobile device management (MDM) system i administrationen af skolens iPads og udrulning af apps og abonnementer. På den måde er skolens iPads også sikret imod misbrug og tyveri. Skolen kan vælge at "fjern-slette" dem, så de ikke kan anvendes til noget af tredjepart. Behovet for en opdateret infrastruktur både fysisk og digitalt bliver løbende afdækket og genovervejet.

Aruba accesspunkter:					
AP105	1		AP-105	19-08-2015	Begrænset livstid
AP105	1		AP-105	21-02-2014	Begrænset livstid
AP105	2		AP-105	28-02-2014	Begrænset livstid
AP105	1		AP-105	27-08-2013	Begrænset livstid
AP105	1		AP-105	22-04-2013	Begrænset livstid
AP105	1		AP-105	11-04-2013	Begrænset livstid
AP105	6		AP-105	04-02-2013	Begrænset livstid
AP135	4		AP-135	04-02-2013	Begrænset livstid
AP105	3		AP-105	19-08-2011	Begrænset livstid
AP105	8		AP-105	03-01-2011	Begrænset livstid
AP105	16		AP-105	29-11-2010	Begrænset livstid
Switche, HP-Aruba:					
1910-8G-POE	5		JG350A	01-12-2014	Begrænset livstid
S1500-24P	1		S1500-24P	14-02-2014	Begrænset livstid
1910-24G-POE	1		JE007A#ABB	13-05-2013	Begrænset livstid
1810-8G	1		J9449A#ABB	19-08-2011	Begrænset livstid
1810-24G	1		J9450A#ABB	19-08-2011	Begrænset livstid
1810-24G	1		J9450A#ABB	21-01-2011	Begrænset livstid
1410-8G	1		J9559A#ABB	21-01-2011	Begrænset livstid
1810-24G	8		J9450A#ABB	03-01-2011	Begrænset livstid
1410-8G	3		J9559A#ABB	03-01-2011	Begrænset livstid
1810-24G	3		J9450A#ABB	29-11-2010	Begrænset livstid
Router:					
HP DL320e v2	1	CZ135101UU	726042-425	31-12-2013	24-01-2015
Servere:					
HP DL320e v2	1	CZ1443005X	726042-425	15-06-2015	23-11-2015
HP ML350G6	1	CZJ1190NRW	470065-334	30-06-2011	13-06-2014
UPS, Batteri backup:					
SMC1500I	3		SMC1500I	21-10-2015	21-10-2017
Projektor:					
EB585Wi	1		V11H600040	04-07-2014	04-07-2016
EB485WI	1		400075	26-03-2013	26-03-2015
EB485WI	1		400075	17-12-2012	17-12-2014
Aruba Controller:					
Aruba 3400	1		3400	17-12-2012	?
Straightshaper:					
S5000U	1		S5000U	29-11-2010	?

Alle skolens iPads udleveres sammen med et cover, der er godkendt af skolens forsikringsselskab. Forsætlige skader dækkes dog ikke. Eventuelle skader, der måtte være påført uden cover, dækkes heller ikke af forsikringen.

Netværksadministratorer kan med mellemrum se systemet efter for at sikre, at det anvendes i overensstemmelse med formålet. Derfor må brugerne acceptere, at beskeder, materiale på hjemmesider og andet arbejde, som gemmes på netværket, kan gennemses.

Pædagogik

Skolen har igennem de senest år haft særligt fokus på at udvikle skolens brug af IT i undervisningen. Siden foråret 2013 har skolen målrettet arbejdet med digitale læringsprocesser med udgangspunkt i forskellige computere og tablets i klasseundervisningen. Fokus har været på forskellige tablets, forskellige læringsplatforme (Learning Management Systems) og digitale læringsressourcer. Grundlaget for denne plan er den efterhånden veludbyggede generelle forskningsmæssige evidens fra arbejdet med informations- og kommunikationsteknologi i skoleverdenen og erfaringer fra en række frontløberskoler i både ind- og udland.

Skolens implementering af en IT-baseret fagdidaktik er opdelt i 3 faser:

1. Almenpædagogiske muligheder og udbytte ved at anvende IT
2. Fagdidaktiske muligheder, hvor IT understøtter fagspecifikke læringsmål
3. En egentlig IT-baseret fagdidaktik

Formål

Formålet med IT i undervisningen og 1:1 teknologi på 1.-6. årgang er, at accelerere elevernes læring. Igennem en synliggørelse af læringsmål skal der sikres et øget ansvar og motivation for læring. Læringsteknologien:

- Støtter elevens læringsituationer i skolen, hjemmet og lektiesituationen.

- Giver læreren mulighed for en øget individuel tilrettelæggelse af undervisningen.
- Giver eleven bedre mulighed for en øget individuel læring generelt.

Mål

1. Bred anvendelse af teknologi. Teknologi skal være et naturligt arbejdsredskab i undervisningen. Det skal anvendes bredt i alle pædagogiske sammenhænge, hvor det didaktisk giver mening.
2. Udvikling af læringsrummet. Læringsrummet skal matche samfundets teknologiske og kompetencemæssige udvikling. Elevernes digitale virkelighed skal inddrages i læringsrummet. Dvs. brugen af forskellige medieplatforme, applikationer m.m. og den interaktion, der finder sted.
3. Læreprocesser understøttes af læringsteknologien. Læringsteknologien skal understøtte læreprocesser, der har fokus på samarbejde, kommunikation og læringsfællesskaber. Læringssynet skal styrke elevernes motivation, nysgerrighed og glæde ved at lære, så de bliver deltagende og producerende i læringsprocessen.
4. Inklusion og undervisningsdifferentiering øges. iPad-ordningen skal give den enkelte elev bedre mulighed for, at lære i det tempo og på den måde, der passer den enkelte bedst. Skolen skal sikre elevernes lige muligheder, for at indgå som deltagere i anerkendende og udviklende fællesskaber.
5. Skole-hjemsamarbejdet styrkes. Elevernes personlige enhed skal gøre elevernes faglige arbejde tilgængeligt såvel i skolen som i hjemmet. Forældre skal stå styrket, ved at have bedre mulighed, for at følge med i skolehverdagen og i den faglige progression.

Interaktive tavler

Hvert læringsrum i skolen, hvor det fagligt kan begrundes, er udstyret med en interaktiv tavle. Den interaktive tavle giver mulighed for at formidle stoffet via mange kanaler, så undervisningsformen bliver varieret og differentieret. Med den interaktive tavle har medarbejderen også mulighed for at tilgodese den enkelte elevs læringsstil

og skabe et flow i undervisningen ved hurtige skift fra tekst til billede til lyd og hermed fastholde opmærksomheden på et fælles oplæg, et fælles tema eller en fælles oplevelse.

Indsats

Udover multimedievejlederen og klasselærerne har skolen nedsat forskellige projekter og teams, der løbende følger udviklingen af brug af IT i de enkelte klasser og på de respektive årgange.

- Pilotprojekter: Der skal igangsættes pilotprojekter, der kan bidrage til at forankre it og læring i skolen, SFO og Klub. Disse kan også medvirke til at skabe videndeling på tværs. Vi går fra bøger i papirformat til at anvende internetportaler, apps og e-bøger.
- Harmonisering af videndelingsplatforme: Der skal etableres en udviklingsgruppe, som skal udvælge en videndelingsplatform, der tilgodeser hele skole- og dagtilbudsområdet.
- Videndeling: Der skal etableres en formaliseret erfaringsudveksling omkring udviklingsprojekter. Det er vigtigt, fordi læring skal være et væsentligt fundament for udviklingsprojekter.
- Teamsamarbejdet: Kollegial og forpligtende faglig videndeling skal formaliseres for at styrke og kvalificere den enkelte leder og medarbejders viden om metodik, digitale læremidler og muligheder.
- Multimedievejlederen: Multimedievejlederen skal have fokus på læreprocesserne, mens de mere tekniske opgaver skal løses af en it-servicemedarbejder.

Retningslinjer

- Eleverne er velkomne til at medbringe IT på skolen.
- Den enkelte lærer bestemmer suverænt, om der må benyttes IT i undervisningen.*

- Såfremt en lærer har bestemt, at der IKKE må benyttes IT i vedkommendes klasse, må denne kun tages frem, såfremt læreren beder om det til løsning af en specifik opgave i en konkret situation.
- IT må alene benyttes til fagligt relevant arbejde i timerne.

*Undtaget herfor er elever med diagnosticeret dysleksi, som benytter "IT-rygsæk" i alle fag.

Retningslinjer iPads

- Eleverne skal medbringe skolens iPad i skole hver dag.
- Eleverne skal sørge for, at skolens iPad er fuldt opladt ved skoledagens start.
- Eleverne skal sørge for, at du har et par høretelefoner med i skole – hvis du har et ekstra sæt, kan du eventuelt have det liggende i klassen.
- Eleverne må ikke tage skolens iPad ud af det cover, som den blev udleveret med.
- Eleverne må ikke tage skolens iPad med ud i frikvartererne.
- Eleverne må ikke spille egne spil, gå på Facebook, Messenger mv. på skolens iPad i timerne uden lærerens tilladelse.
- Eleverne skal prioritere det faglige indhold højere end det private i tilfælde af pladsmangel på skolens iPad.
- Eleverne skal gå ind i "indstillinger" og slå "Tillad meddelelser" fra i alle applikationer på skolens iPad, så du ikke forstyrres i undervisningen.
- Eleverne skal sørge for, at sikre skolens iPad bedst muligt.
- Eleverne skal sørge for, at tage backup af dit indhold på skolens iPad.

Sanktioner

- Anvender eleven IT i strid med disse retningslinjer, inddrager læreren/medarbejderen enheden og afleverer den på skolens kontor snarest herefter samme dag. Eleven kan efterfølgende få enheden udleveret, når skoledagen er slut.

- Hvis eleven gentagne gange overtræder disse regler, tager en person fra skoleledelsen kontakt til forældrene for at finde en løsning på problemet sammen med dem og eleven.

Adfærd

Brugeren skal behandle andre mennesker på nettet, deres indlæg samt selve nettet med respekt. De skal sørge for at egne indlæg altid kan "tåle" at blive set på tryk i underskrevet stand. Uden for undervisningen er det tilladt at benytte IT til privat brug. Brugere skal så vidt muligt undgå unødige udskrivinger på papir set ud fra et både økologisk og økonomisk hensyn.

Eksempler på uacceptabel adfærd

- Brugeren må ikke ændre maskinens opsætning uden at det er aftalt med en af multimedievejlederen først.
- Netværket må ikke bruges til kommercielle formål. Brugere må ikke købe eller sælge produkter eller serviceydelser via nettet uden forudgående tilladelse fra ledelsen.
- Brug af netværket i forbindelse med politisk og racistisk agitation er forbudt. Brug af netværket i forbindelse med områderne vold og pornografi er forbudt. Brugere må heller ikke kontakte websites, nyhedsgrupper eller chat-fora, som indeholder materiale, der er obscønt, eller som opfordrer til ulovlige handlinger.
- Netværket må ikke bruges til nogen form for aktivitet, i forbindelse med udbredelse af materiale, der er forbudt i følge dansk lovgivning, herunder regler og love om ophavsret.
- Det er ikke tilladt brugere at anvende vulgært, nedsættende eller obscønt sprog på nettet. Det er også forbudt at fremkomme med personlige angreb, at chikanere andre personer eller offentliggøre private oplysninger om en anden person.
- Brugere må ikke logge på med en anden persons identitet eller forsøge at få adgang til andre brugeres filer. Det er også forbudt at tvinge sig adgang til andre personers eller organisationers computersystemer gennem f.eks.

"hacking" eller på anden måde. Brugeren må ligeledes heller ikke skjule sin identitet, bortset fra de tilfælde hvor det eksplicit er tilladt.

- Brugere må ikke "spamme" (sende uhensigtsmæssig mange e-mail af sted på én gang). Vold, hærværk og tyveri imod skolens materiel er forbudt.

Vedvarende proces

IT-sikkerhedspolitikken kræver løbende opfølgning og opmærksomhed fra både bestyrelse, ledelse, elever, forældre og medarbejdere, hvis visionen skal lykkes.

Ledelsen har en særlig betydningsfuld rolle. Lederteamet skal sammen med udvalgte ressourcepersoner gå forrest i forhold til den digitale udvikling. De skal sætte IT på dagsordenen på alle niveauer og skabe sammenhæng mellem skolens mål og nærværende politikker.

Forældrene har også en central rolle i at understøtte deres børns IT-kompetencer i fritiden, og i det hele taget være en del af børnenes og de unges virtuelle liv. Forældrene bør f.eks. bevidstgøre deres børn om tiden, de bruger på nettet, deres færden på nettet og brugen samt misbrugen af sociale medier.