IT Sikkerhedspolitik

Indledning
Dette dokument fastsætter hovedprincipperne i skolens sikkerhedspolitik. Herudover skal der laves forskellige instruktioner og vejledninger, der tager udgangspunkt i nedenstående.

Sikkerhedspolitikken omfatter såvel elevnettet som det administrative-/lærernettet.

Fysisk sikkerhed
Nyborg Friskole ønsker i videst muligt omfang at sikre de fysiske installationer mod ulykker, hærværk og tyveri. Ligeledes sikres i størst muligt omfang mod forsyningssvigt i serverrum.

Datasikkerhed
Administrative data repræsenterer en betydelig værdi og skal sikres mod uautoriseret adgang, tab og forvanskning. IT-sikkerhedsudvalget fastsætter sikkerhedsniveauet for de enkelte systemer, herunder klassificering af data og vurdering af, hvorvidt et egentligt nødberedskab skal etableres.

Sikkerhedsudvalget etablerer procedurer for logning, brugeradministration, e-mail politik og anvendelse af internet.

Ligeledes sikres at backup-procedurer og viruspolitik overholdes.

IT-anvendelsespolitik for Nyborg Friskole
Formålet med at etablere en IT-anvendelsespolitik er, at skabe en forståelse hos skolens medarbejdere og elever for hvorledes skolens IT-udstyr tænkes anvendt.

Det er Nyborg Friskoles ønske at give medarbejdere og elever gode muligheder for brug af IT-faciliteter uden brug af unødvendige restriktioner men samtidigt sikre mod misbrug af vore systemer eller misbrug udført herfra af andre systemer.

Nyborg Friskole ønsker med sin anvendelsespolitik at præcisere.

- Alle skolens computere på områder er undervisningsmidler - på linje med andre undervisningsmidler.
- Undervisningsrelateret arbejde på internet har altid fortrinsret frem for planløs surfen og "privat chat".
- Computere på skolen må gerne benyttes til andet end undervisningsformål, når blot anvendelsespolitikken overholdes.
- Ligeledes må egne computere gerne benytte skolens trådløse net, hvis bare anvendelsespolitikken overholdes.

Acceptabel brug af IT-miljøet.
IT-miljøet bruges i forbindelse med undervisnings- og aktivitetsrelevant arbejde på skolen. Herved forstås f.eks. indsamling og fremlæggelse af data i undervisningssituationer samt udveksling af projektrelaterede ideer, meninger og spørgsmål ved hjælp af e-mail, præsentationer eller lignende.

Ansatte og elever har pligt til at holde deres adgangskodeord hemmeligt. Brugerrettigheder og adgangskodeord må ikke deles med andre.

Udvis netetik. Det betyder at brugeren behandler andre mennesker på nettet, deres indlæg samt selve nettet med respekt. Sørg f.eks. for at egne indlæg altid kan "tåle" at blive set på tryk i underskrevet stand.

Undgå unødig udskrivning. Tænk både økologisk og økonomisk.

Arbejdsstationer (tavlecomputere, PC'ere i personaleforberedelsen etc.) skal, når de forlades efter endt session, logges af mail, intranet mm.

Eksempler på uacceptabel brug af skolen computere

- Brugeren må ikke ændre maskinens opsætning uden at det er aftalt med IT-medarbejderen. (medarbejdercomputere er her undtaget)
- Det er ikke tilladt at downloade, kopiere, installere eller gemme software, shareware eller freeware i nogen form uden tilladelse fra IT-medarbejderen. (medarbejdercomputere er her undtaget)
- Netværket må ikke bruges til kommercielle formål. Brugerne må ikke købe eller sælge produkter eller serviceydelser via nettet uden forudgående tilladelse fra IT-medarbejderen.
- Brug af netværket i forbindelse med politisk og racistisk agitation er forbudt.
- Brug af netværket i forbindelse med områderne vold og pornografi er forbudt.
- Brugerne må ikke kontakte web-sites, nyhedsgrupper eller chat-fora, som indeholder materiale, der er obskønt, eller som opfordrer til ulovlige handlinger.
- Netværket må ikke bruges til nogen form for aktivitet, i forbindelse med udbredelse af materiale, der er forbudt ifølge dansk lovgivning, herunder regler og love om ophavsret.
- Det er ikke tilladt brugere at anvende vulgært, nedsættende eller obskønt sprog på nettet. Det er forbudt at fremkomme med personlige angreb, at chikanere andre personer eller offentliggøre private oplysninger om en anden person.
- Brugerne må ikke logge på med en anden persons identitet eller forsøge at få adgang til andre brugeres filer. Det er 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.
- Brugerne må ikke "spamme" (sende uhensigtsmæssig mange e-mail af sted på én gang).
- Vold, hærværk og tyveri imod skolens materiel er forbudt.

Medarbejdercomputere
Medarbejdercomputere skal være forsynet med password. Hvis der tillades flere brugere på computeren, må der ikke være adgang til personfølsomme oplysninger. Husk i dette tilfælde at computeren ikke må gemme adgangskoder til automatisk indlogning.

Der skal være installeret anti-virus (af skolen stillet til rådighed).

Passwordsikkerhed
Når du som underviser får adgang til it-systemer og data, får du samtidig adgang til en række ressourcer og oplysninger, som er fortrolige og strengt personlige. Derfor bliver alle it-brugere udstyret med et hemmeligt og personligt password, som ikke må videregives til andre, heller ikke dine nærmeste kolleger.

En udlevering af password ville ansvarsmæssigt svare til, at du udleverede dit Dankort og din pinkode til en kollega. - Du hæfter personligt for den anvendelse / misbrug dette giver mulighed for. Password må ikke oplyses til eksterne teknikere eller eksternt servicepersonale, og password må ikke kommunikeres / udleveres i forbindelse med henvendelser på e-mail.
For at passwords skal have den ønskede effekt, er det nødvendigt at stille visse minimumskrav til opbygning og længde samt ændringsinterval. Et godt password er en bogstav- / talkombination, som er nem at huske, men til gengæld er svær at gætte for andre. Undgå specialtegn som #, ¤, /, @ og lignende, da det i nogle henseender kan give problemer. ***Undgå også Æ, æ, Ø, ø, Å, å,*** da det er specielle danske bogstaver, som kan give systemmæssige problemer.

Anvend derfor kun tal samt de 25 første bogstaver i alfabetet. Anvend aldrig eget navn, egne eller den nærmeste families initialer, fødselsdag, bilnummer, hundenavn eller lignende, da det er oplagt at prøve den slags kombinationer for uvedkommende.
Gode passwords er oftest opbyggede af tal- og bogstavkombinationer – gerne med både store og små bogstaver. Et godt password skal indeholde min. 8 tegn.

Sikkerhed imod virus
Virus kan overføres via USB-stik, via CD-rom, eller via Internettet og e-mail etc. For at undgå virus, er alle computere forsynet med et antivirusprogram.

For at minimere risikoen for, at din pc bliver inficeret med virus, kan følgende huske-regler skitseres:

- Undgå uautoriserede programkopier, såkaldte piratkopier.
- Der må aldrig være en USB nøgler eller CD i pc'en, når den tændes.
- Benyt aldrig data fra CD'er, USB nøgler og disketter, hvor oprindelsen ikke kendes.
- Kør en viruskontrol på din pc, hvis du har mistanke om, at uautoriserede brugere har benyttet den.

Har din maskine fået virus, skal du fysisk afbryde forbindelsen til netværket (almindeligvis slukke for systemet) for at undgå, at virus spredes yderligere. Herefter ***skal*** du kontakte skolens IT-personale.
Det er **ikke** flovt at have fået virus på sin maskine. - Du behøver derfor **ikke** at holde det hemmeligt!

Udskrivning
Som it-bruger udskriver du ofte dokumenter, notater og lignende - enten dine egne eller andres. Disse dokumenter kan være fortrolige, hvorfor de skal behandles med rette omhu. Du er ansvarlig for at behandle fortrolige udskrifter, så de ikke kommer i de forkerte hænder. Du må derfor kun udskrive på en printer, hvor du er ved siden, af så udskriften ikke kan tilgås af andre end dig selv. Fortrolige dokumenter indeholder ikke nødvendigvis personfølsomme oplysninger.

Afsendelse af fortrolige og personfølsomme oplysninger
Er karakteren af kommunikationen således, at oplysningerne, der sendes, er fortrolige eller personhenførbare, **må man ikke sende en almindelig e-mail.**

Du skal enten sende dokumenterne pr. alm. brevpost eller sende en via sikker e-mail.

Opskrivning

Husk at være i god tid!

Det er en god idé at skrive jeres barn op i meget god tid, da Nyborg Friskole er en populær privatskole med ventelister på de fleste klassetrin.

Opskrivning kan ske ved at bruge ventelisten på hjemmesiden www.nyborgfriskole.dk findes under indmeldelse.

Optagelse vil kun ske efter en personlig samtale med skolen.

Betingelser for opskrivning
Opskrivning gælder, indtil I bliver tilbudt en plads. Bliver I tilbudt en plads, men takker nej, er det

muligt at fortsætte på ventelisten, men opskrivningsdatoen vil blive ændret til den dato, hvor man takker nej. Det vil altså have indflydelse på ventelisteplaceringen.

Skolen oplyser ikke den eksakte ventelisteplacering, idet der er flere kriterier, der gør sig gældende for den enkelte elevs mulighed for optagelse - bl.a. antallet af søskendebørn på ventelisten, kønsfordeling i klasserne o.a.

Det er vigtigt at holde os ajour med mail-adresser og mobilnumre. Korrektioner til opskrivning foretages ved at logge på ventelisten med NemID. Ventelisten findes på vores hjemmeside under indmeldelse.

OPSKRIVNING KAN IKKE GENNEMFØRES UDEN FULDE OG KORREKTE CPR-NUMRE PÅ BÅDE ELEV OG FORÆLDRE

Vær opmærksom på at udfylde opskrivningsår og -klasse korrekt. Det er på eget ansvar, at barnet bliver noteret på den rigtige venteliste.

Børn skal som udgangspunkt starte i skole i det kalenderår, de fylder 6 år - f.eks. er barnet født i 2014, skal det skrives op til skolestart i skoleåret 2020/21.

Fortrolighedspolitik
Skolen forstår og respekterer vigtigheden af privatliv på internettet. Skolen vil ikke afsløre information om brugere til tredjepart, med mindre det er nødvendigt for at implementere en transaktion. Skolen vil ikke sælge dit navn, adresse, kreditkort eller personlige data til nogen tredjepart uden din forudgående tilladelse.

Nyborg, den 25. april 2018