

IT sikkerhedspolitik for elever på Øregård Gymnasium

Indledning

Denne politik er lavet med elevrådet som primær afsender og er godkendt af skolens ledelse.

Ønskes IT sikkerhedspolitikken ændret, tages dette op i elevråd samt hos skolens ledelse.

Formålet med politikken er at sikre, at vi alle sammen har et netværk, som vi kan bruge sikkert i det daglige arbejde og til de sociale medier i pauserne.

Vi vil stå sammen om at holde dem ude, der har til hensigt at ødelægge og misbruge vores fælles netværk.

Ved at vi overholder nogle få regler og retningslinjer, samt tale om it-sikkerhed, får vi nogle kompetencer, der er efterspurgt af samfundet nu og i fremtiden.

Der skelnes i denne politik mellem regler og retningslinjer.

- Regler skal overholdes, og brud kan medføre sanktioner.
- Retningslinjer bør følges, for at vi alle sammen får en høj sikkerhed på vores netværk.

Er du i tvivl, så spørg en klassekammerat, en underviser eller en fra ledelsen.

Passwords (retningslinje)

I dag gælder det om at have et rigtig langt password, som er dedikeret til de enkelte services (facebook, twitter, lectio ect.), som man logger på. Et 8-tegns password kan crackes på under 8 timer, selvom man har brugt specialtegn og tal. Man kan let lave et sikkert password, der er til at huske på følgende måde:

– lav en sætning:

“jegelskeratspiseburgers”

– lav noget der er forskellig fra service til service:

“jegelskerFBatspiseburgers” (for FaceBook password)

– hvis du vil lave ekstra sikkerhed, så gør f.eks. hvert andet bogstav stort og tilføj et tal eller specialtegn:

“jEgeLskerFBaTsPisebUrgers 1”

Surfing på internettet (regel og retningslinje)

Regel: Der må ikke surfes på sider eller købes tjenester, der er i strid med dansk lovgivning (f.eks. BitTorrents (download af ulovlig musik/film), hackersider, der tilbyder at lægge netværket ned, virusbefængte sider, hvor dette er åbenlyst etc.)

Retningslinje: Brug din sunde fornuft, når du surfer på internettet. Besøg kun sider der er relevante for dit studie, eller sider som er anerkendte som f.eks. Twitter og Facebook.

Brug af sociale medier (regel og retningslinje)

Regel: Det strider mod dansk lovgivning at udgive sig for en anden og poste noget via en andens facebookprofil.

Ligeledes gælder det, at man kan straffes med bøde og op til 6 måneders fængsel (§ 264d), hvis man poster billeder af en anden mod dennes vilje. Dette gælder billeder, som er taget i et ikke-offentligt rum – f.eks. til en privat fest.

Ligeledes kan man straffes endnu hårdere efter loven om børneporno (§ 235), hvis man besidder eller formidler nøgenbilleder af personer under 18 år.

Retningslinje: Når først noget er på internettet, kan det ikke slettes, og du kan komme til at skade både dine venner og skolen ufrivilligt. Tænk dig om, før du poster noget om dig selv, andre eller gymnasiet – **husk der er et menneske bag det du poster.**

Beredskab: Er man blevet krænket på nettet, skal man omgående kontakte it-chefen (LP) eller vicerektor (BG) som kan hjælpe med at begrænse skaden mv.

Upload og download (regel)

Brug af BitTorrents er ikke lovligt. BitTorrent er programmer, der bruges til at dele ulovligt indhold – typisk film og musik, men også ulovlige filer. Samtidig hermed er programmerne en stor kilde til malware som f.eks. virus, samtidig med at de er en stor belastning for det fælles netværk.

Eksempler er:

Piratebay, Kickasstorrents, Torrentz, Ekstratorrent, yify-torrent, EZTV, 1337x, Isohunt.to, Bitsnoop, Rarbg.

Overvågning (regel)

Gymnasiet overvåger som udgangspunkt ikke personlige forhold, eller hvad man skriver på de sociale medier, i mails, chats eller hvad der søges på. I forbindelse med eksamen sker der dog en kontinuerlig overvågning, der kan vise om der anvendes sider eller programmer, der strider mod denne it-sikkerhedspolitik.

I forbindelse med eksamen:

- enheder der bruges i eksamenssammenhæng kan udtages til kontrol
- enheder der bruges i eksamenssammenhæng overvåges

Hacking (regel)

Forsøg på hacking af enheder på netværket er i strid med dansk lovgivning. Hvis du undersøger, eller forsøger at få adgang til en andens enhed på netværket, er der tale om hacking.

Antivirus/malwarebeskyttelse (regel)

Uanset om du bruger mac eller pc, skal du have installeret et antivirus-/malware-beskyttelsesprogram.

Vi anbefaler Avira til mac/pc eller Sophos antivirus kun til mac, som begge er gratis pt.,

Sanktioner

Overtrædelse af reglerne i denne it-sikkerhedspolitik kan medføre forskellige former for sanktioner - i værste fald politianmeldelse og bortvisning. Ved en overtrædelse vil en it-ansvarlig dog først gå i dialog med eleven og den pågældendes forældre - såfremt eleven er under 18 år - inden sanktionen iværksættes.

Godkendt af Elevrådet 2016/17