JAKOBSBERGS
FOLKHÖGSKOLA

# IT-Policy för Jakobsbergs folkhögskola

Antagen 2018-04-03 - Uppdaterad 2018-05-24

# Inledning

Det här dokumentet beskriver regler och riktlinjer för användningen av IT-resurser inom Jakobsbergs folkhögskola. Med IT-resurser menas datorer, nätverk, system och all annan kringutrustning som används i samband med hantering av information i digital form.

Reglerna gäller alla anställda, deltagare och samtliga övriga användare av skolans IT-resurser som t.ex. praktikanter och externa konsulter.

Avsikten med dokumentet är att skydda skolans verksamhet, deltagare, kunder, partners, anställda och andra intressenter. Denna policy ersätter alla tidigare policys på området och kommer att bli föremål för tillägg och förändringar när så krävs.

Den grundläggande princip på vilken dessa regler och riktlinjer vilar, är att skolans IT-resurser ägs av skolan och utgör ett arbetsredskap som skall användas för skolans verksamhet. Skolan ska inte lida skada eller få onödiga kostnader genom olämplig användning av dessa arbetsredskap.

Skolans IT-resurser får inte användas för att på otillbörligt sätt sprida, förvara eller förmedla information:

- i strid mot gällande lagstiftning, t.ex. hets mot folkgrupp, barnpornografibrott, olaga våldsskildring, förtal, ofredande, dataintrång eller upphovsrättsbrott
- som är att betrakta som politisk, ideologisk eller religiös propaganda
- i strid mot dataskyddsförordningens (GDPR) stadgar om den personliga integriteten
- som i annat fall kan uppfattas som kränkande och stötande
- som syftar till att marknadsföra produkter eller tjänster som saknar anknytning till skolan
- som på något annat sätt kan störa skolans IT-verksamhet.

# Individuellt ansvar

Det är viktigt att alla berörda inser det individuella ansvar som denna policy innebär. Som användare förväntas du känna till och följa dessa regler och riktlinjer. Det är också viktigt att användandet av skolans IT-resurser görs på sådant sätt att skolans namn, anseende och goda rykte bibehålls.

# Behörighet

Behörigheten till skolans IT-resurser är personlig och får inte överlåtas eller på annat sätt göras tillgänglig för annan anställd eller extern part. Det är inte tillåtet att nyttja någon annans behörighet eller utnyttja felaktiga konfigurationer, programfel eller på annat sätt manipulera skolans IT-resurser.

# Säkerhet

För att skydda mot spridning av virus och mot obehörigt tillträde skyddas våra IT-resurser av säkerhetssystem, såsom antivirusskydd och brandväggar. Det är inte tillåtet att avaktivera eller på något sätt manipulera dessa skydd.

Alla anslutningar och installationer av datorer eller annan utrustning i skolans nätverk ska utan undantag godkännas av skolans IT-ansvarige.

Användaren är ansvarig för en säker användning av sin personliga utrustning och att vidta alla rimliga åtgärder för att skydda IT-resurser mot virus, obehörigt tillträde eller andra attacker mot systemets säkerhet och integritet.

För att förhindra obehörig åtkomst till information, har skolan valt att via policy automatiskt aktivera lösenordskyddad skärmsläckare efter 15 minuters inaktivitet av datorn.
Bärbara datorer ska om möjligt vara inlåst nattetid i avsett utrymme på skolan, alternativt tas med hem.

# Brandvägg

Skolans brandvägg blockerar all trafik som inte medvetet är tillåtet. Det innebär att nya tjänster inte kommer fungera förrän portar och IP-adresser öppnats upp.

Endast tjänster som är relevanta för utbildningen tillåts. Allt annat såsom onlinespel kommer inte att tillåtas.

# Backup och återställning (se även lagring)

I största mån skall dokument förvaras i molntjänsten Google Drive där Google sköter backupen. De dokument och filer som inte sparas på Google Drive skall sparas i det lokala nätverket, OES Micro Focus tidigare Novell.

Med tjänsten/programmet Micro Focus Filr synkas automatiskt filer mellan den lokala datorn och nätverket. Med denna tjänst finns alltid en backup av alla personliga filer som sparas i mappen Micro Focus Filr.

Säkerhetskopior av Vismas löne- och administrationsfiler måste även sparas med den regelbundenhet som erfordras på USB-minne och förvaras inlåst i brandskyddskåp.

IT-ansvarig tar backup av alla dokument som sparas i det lokala nätverket med jämna mellanrum. Backupen av dina filer lagras i en annan byggnad än där filservern finns.

# Lösenord

Lösenord och användaridentitet ska ses som personliga uppgifter och får inte lämnas ut till någon annan. Lösenord skall av användaren omgående bytas om misstanke finns att det har avslöjats. IT-ansvarig förbehåller sig rätten att omedelbart byta en användares lösenord vid misstanke om att lösenordet avslöjats. Lösenord bör inte lagras fysiskt t.ex. i pappersform eller digitalt i t.ex. mobiltelefon.

Användare får inte använda samma lösenord till externa system eller för privat bruk (t.ex. Facebook och Gmail) som till skolans resurser.

Lösenordet skall bestå av minst 8 tecken och måste innehålla följande:

- minst en siffra (0-9), minst en stor bokstav (A-Z), minst en liten bokstav (a-z) eller ett specialtecken
- Lösenord bör inte innehålla å, ä, ö eller andra bokstäver som ej finns i det engelska alfabetet
- Lösenord får inte innehålla mellanslag
- Lösenord får inte innehålla delar av ert namn eller kontonamn
- Lösenord får inte innehålla delar av skolnamnet.
- Lösenordet ska bytas minst 1 gånger om året (tvingande)
- Lösenord som tidigare använts får inte sättas till nya lösenord (modifikationer tillåts)

Detta gäller på enheter eller system som har stöd för detta. För mobiltelefoner och handhållna enheter gäller sifferkod, eller om detta inte finns, högsta möjliga säkerhet som enheten har stöd för.

# Lagring

Användare är skyldiga att lagra sina dokument och filer på Google Drive eller på skolans nätverk (Micro Focus Filr). Under inga omständigheter får informationen lagras endast lokalt på den egna datorn. Data som lagras på annat sätt t.ex. Dropbox berörs inte av skolans backup-plan. Eget ansvar gäller då.

**Lagring av filer med persondata - GDPR**

1. Grundprincipen för filer med persondata är att de inte får laddas ned till den lokala datorn eller mobiltelefonen/läsplatta eller liknande enhet eller exporteras ut. Datan skall ligga lagrad i molntjänsterna: Schoolsoft alt. i Google Drive.
2. Persondata från ekonomisystemet Visma skall stanna kvar i programmet.
3. Om persondata laddas ned eller exporteras ut skall de raderas så fort syftet för användningen är utfört.
4. Inga filer med persondata från tidigare terminer än den innevarande får lagras lokalt.

# Kopiering och utskrift

Det är fritt att använda skolans skrivare/kopiatorer så länge det sker inom ramen för utbildningen eller skolans verksamhet. Endast ett fåtal privata utskrifter får göras. Vill man skriva ut större volymer skall man kontakta IT-ansvarig innan utskriften görs.
I februari 2018 togs ett nytt kopiering- och utskriftssystem i drift, PaperCut. Systemet räknar all kopiering och alla utskrifter.

# Internet

Internet är avsett att användas för informationssökning och andra relevanta ändamål inom och för skolans verksamhet.

Vid användning av Internet är det förbjudet:

- att besöka webbsidor med pornografiskt, rasistiskt eller annat innehåll som kan väcka anstöt, undantag kan göras men då i samråd med lärare eller ledningsgrupp
- att ”ladda ner” program och filer om de kan påverka IT-säkerheten på skolan, vid osäkerhet kontakta IT-ansvarig
- att sprida och/eller förfoga över upphovsrättsligt skyddat material utan rättighetsinnehavarens tillstånd
- att besöka spelsidor, spela förströelsespel, använda chatprogram eller liknande i annat syfte än vad som direkt kan kopplas till anställning, projekt eller uppdrag

# E-post

E-post är avsedd att användas för intern och extern kommunikation. All e-post kommunikation som avser skolans verksamhet skall ske genom skolans e-postkonton där det klart skall framgå för mottagaren att mejlet kommer från skolan.

All e-post som skickas till mer än en mottagare förutom till personal skall hemlig-kopia användas.

Användare får inte använda en företagsadress på ett sätt eller i ett sammanhang som kan skada skolans image och anseende. E-post får inte användas för politiska, kommersiella eller andra syften som strider mot skolans verksamhet. E-posten får inte användas för privat bruk, användas i privata diskussionsgrupper, som mottagaradress för privat reklam eller på andra sätt som kan skada företaget.

# Mobiltelefoni

Det är av yttersta vikt att den anställde hanterar sin mobiltelefon med största varsamhet och försiktighet med tanke på vilka säkerhetsrisk denna typ av utrustning innebär, då man via enheten har full tillgång till känslig deltagarinformation.
Den anställde som har en företagstelefon är skyldig att alltid ha telefonen med sig under arbetstid samt använda sig utav växelapplikationen för att ange sin status (t.ex. om man är upptagen i möte).

Geografisk spårning av skolans mobiltelefoner skall vara aktiverat då den kan hittas vid förlust eller annan speciell händelse.
Vid tjänstgöring i utlandet skall uppkoppling ske via Wifi i största möjliga utsträckning.
Vid utlandsvistelse i privat regi får inga kostnader kopplade till skolans mobilabonnemang belasta företaget.
Privata köp t.ex. Blocket eller insamlingar skall helst, om det går göras på annat sätt än vi telefonen. Skulle det inte vara möjligt och köp görs dras kostnaden från lönen.

# Övrig programvara

Användare får inte ladda ner annan än av IT-avdelningen godkända programvaror.
Inga hemsnickrade programvaror får användas på skolans datorer eller i dess IT-miljö.

# Privat användning av IT-resurser

Användare har fått tillgång till IT-resurser för att underlätta deras arbete för företaget och resurserna får inte missbrukas. Emellertid är privat användning acceptabelt under förutsättning att:

- Användningen inte stör några direkta eller indirekta åtaganden med eller för företaget
- Användningen inte medför några kostnader för företaget
- Användningen följer reglerna i denna policy

# Fjärråtkomst

Skolan tillhandahåller fjärråtkomst till sina IT-resurser för de medarbetare som har det behovet.
Det åligger användaren att säkerställa att de datorer som används för fjärråtkomst lever upp till de krav som ställs för god IT-säkerhet (avseende antivirus, personlig brandvägg med mera). Vid osäkerhet om så är fallet skall användaren först stämma av detta med IT-ansvarig.

# Kontroll och övervakning av IT-system

Användare som vid användande av skolans IT-resurser upptäcker fel eller annat som kan vara av betydelse för IT- driften inom skolans, är skyldig att genast rapportera detta till IT-ansvarig.

IT-resurserna övervakas kontinuerligt och händelser på det lokala nätverket loggas. Dessa loggar sparas och arkiveras och kan vid behov utgöra bevis för eventuella överträdelser.

Användning av IT-resurser kan granskas och övervakas i alla situationer där det enligt företagsledningen finns legitim anledning, detta gäller även filer och lagrade meddelanden. Granskning och övervakning får ske utan underrättelse eller begäran om tillstånd.
Skolan kan tvingas göra lagrad information tillgänglig för tredje part som en följd av rättsliga krav eller genom krav från myndigheter.

Övervakningen och kontrollen av resultatet från övervakningen kommer endast att utföras av ett begränsat antal personer.

# Påföljder vid överträdelse

Anställd inom företaget eller annan berörd som på något sätt bryter mot denna IT-policy kommer att ställas till svars för den överträdelse som begåtts. Överträdelsens art styr påföljden men denna kan vara muntlig eller skriftlig varning samt i grova fall avsked från företaget. Användare som misstänks för brott enligt brottsbalken kan bli föremål för polisanmälan.

# Överenskommelse

Härmed intygar jag att jag har läst, förstått och att jag kommer att följa skolans IT-policy. Jag förstår att det åligger mig att använda skolans IT-system på ett sätt som gagnar skolan, dess verksamhet samt dess anställda och deltagare och att den information som jag hanterar via skolans IT-system inte är privat.

Jag förstår också att överträdelser mot denna IT-policy kan leda till disciplinära påföljder och vid grov överträdelse även avsked från företaget. Jag förstår också att denna IT-policy kommer att förändras under dess livscykel för att möta de framtida krav skolans IT-system ställs inför.

**När jag tagit del av Jakobsbergs folkhögskolas Integritetspolicy för deltagare har jag också tagit del av denna IT-policy.**