ALE KOMMUN

# Informationssäkerhet

Riktlinjer för användare

Fastställd av kommundirektören 2011-06-20

# Innehåll

# 1 Informationssäkerhet

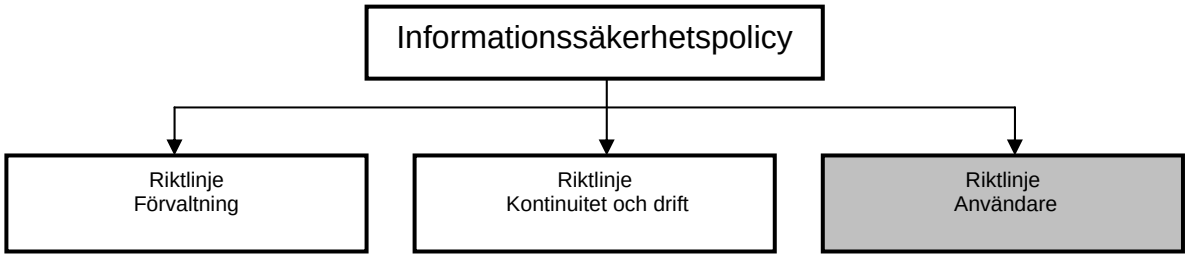
Stora delar av de verksamheter som drivs av Ale kommun är beroende av IT-stöd (IT betyder informationsteknik). Hur vi hanterar informationen som finns i våra datasystem och nätverk är av största vikt för kommunens arbete.

Både samhället i stort och kommunens medborgare ställer höga krav när det gäller skydd för den personliga integriteten och tillförlitlighet i kommunens system. Kommunen har en samhällsviktig roll och verksamheten ska fungera såväl till vardags som vid kris. För att klara detta krävs ett genomtänkt och kontinuerligt säkerhetsarbete.

För att vi ska kunna hålla rätt säkerhetsnivå är det viktigt att du som användare känner till kommunens policy och regler.

Informationen måste alltid finnas när du behöver den och du måste kunna lita på att den alltid är korrekt. Därför måste du skydda dig mot förlust av information, men också mot oavsiktlig eller obehörig ändring av den. Informationssäkerhet innebär också att de som inte är behöriga inte ska få tillgång till information.

Arbetet med informationssäkerhet i Ale kommun styrs av flera dokument: informationssäkerhetspolicy och riktlinjerna för informationssäkerhet som gäller systemförvaltning, kontinuitet och drift samt den här riktlinjen som är till för dig som användare:




I den här riktlinjen får du veta vad du som användare ska tänka på för att vi ska hålla en god säkerhetsnivå i Ale kommun.

# 2 Organisation och ansvar

## 2.1 Informationssäkerhetssamordnare

Ha huvudansvaret för samordning av informationssäkerhetsarbetet.

- Ansvara för att övergripande policy och riktlinjer för informationssäkerhetsarbetet utarbetas och beslutas.
- Övervaka att policy och riktlinjer för informationssäkerhetsarbetet följs och vid behov föreslå förbättringar.
- Ta initiativ till och medverka i informations- och utbildningsaktiviteter gällande informationssäkerhet.
- Kontrollera att befintliga säkerhetsregler följs och vid behov föreslå förbättringar
- Initiera informationssäkerhetsrevisioner.

## 2.2 IT-chef

IT-chefen är systemägare för det interna IT-nätverket och har ansvaret för att detta och IT-systemens tekniska delar fungerar. IT-chefen ansvarar för att identifiera de delar som ingår i det interna IT-nätverket samt att en säkerhetsanalys genomförs. IT-chefen ansvarar också för att riktlinjen Kontinuitet och drift följs och uppdateras samt att en kontinuitetsplan för driften av IT-verksamheten upprättas och att den senare integreras med Ale kommuns gemensamma kontinuitetsplan.

## 2.3 Sektorschef

Det operativa ansvaret för att datasystemen uppfyller verksamhetens krav vilar på sektorschef. I detta ansvar ingår att bedöma verksamhetens krav på säkerhet avseende sekretess, tillförlitlighet, tillgänglighet, spårbarhet samt att personalen har tillräckliga kunskaper för att hantera IT-systemet på ett säkert sätt.

## 2.4 Systemägare

Systemägare är sektorschef/verksamhetschef. Denne är ytterst ansvarig för systemets användning, ändamål, säkerhet, budget samt organisation för systemförvaltning. Systemägare fattar beslut inom ramen för antagna mål och resurser om de egna IT-systemens införande, drift, förvaltning och avveckling. Systemägaren ska i samråd med både sektorschef och applikationsansvarig upprätta regler för tilldelning av behörigheter.

Systemägaren utser applikationsansvarig.

## 2.5 Applikationsansvarig

Applikationsansvarig ska inom givna ekonomiska ramar operativt sköta systemets förvaltning. I uppdraget ingår att se till att det finns en praktiskt fungerande förvaltningsorganisation, ansvara för utbildning, systemdokumentation och anpassningar/utveckling av systemet.

### 2.6 IT-samordnare

- Samordnar informationssäkerhetsarbetet i egen sektor/del av sektor med utarbetade rutiner.
- Koordinerar och utbildar i/kring informationssäkerhet för nyanställda på den sektor man ansvarar för.
- Beställer nya konton för nya användare samt grupprättigheter.
- Ser till att en förteckning över användare och rättigheter förs och följer regelbundet upp dessa.

### 2.7 Användare

Användare är varje person som använder ett IT-system tillhandahållet av Ale kommun.

Ansvarar för att följa kommunens gällande policy och riktlinjer för informationssäkerhet och för respektive IT-system.

### 2.8 Definition Applikation - system

**Applikation** är en typ av datorprogram som fyller ett direkt syfte för användaren. En applikation kan exempelvis vara nyttoprogram som Microsoft Word och Excel, kommunikationsprogram som Outlook, webbläsare som exempelvis Internet Explorer eller nöjesprogram som datorspel och mediaspelare.

En applikation som ansluter mot någon form av databas eller server kallas ofta för **IT-system** eller bara **system.** Exempel på sådana system är E-post ystemet Exchange, ett lönesystem eller ett journalsystem.

# 3 Vem ska komma åt information i datasystemen?

## 3.1 Behörighet

Kommunens IT-system (datasystem) har olika berörighetsnivåer. Behörigheterna styr vilken rättighet du har att utnyttja systemet och den information som finns i det. Varje gång du använder kommunens datorer eller nätverk görs en automatisk kontroll av din behörighet och det du gör registreras (loggas).

Alla användare får en behörighet för inloggning till nätverket och till olika IT-system inom kommunens nätverk. Din behörighetsnivå styrs av vilken arbetsuppgift/roll du har och vilken information du behöver för att utföra dina arbetsuppgifter.

För att få tillgång till vissa specifika IT-system behövs ett godkännande från din chef.

Din behörighet beställer du hos din sektors IT-samordnare efter godkännande av ansvarig chef.

Förtroendevalda har inte på grund av sin ställning som ledamot i en nämnd befogenhet att ta del av handlingar som inte är allmänna. Den befogenhet som enligt kommunallagen tillkommer nämnden kan inte anses tillkomma envar enskild ledamot i nämnden.

Nämndordföranden förutsätts dock inför nämndsammanträde ha tillgång till den information som ordföranden behöver för att kunna upprätta kallelse till nämnden med tillhörande föredragningslista och övriga sammanträdeshandlingar som ofta inte är allmänna handlingar.

Mellan sammanträdena gäller således samma regler för utlämnande av handlingar till nämndledamöterna som till allmänheten.

Grundläggande IT[1]-behörighet tilldelas förtroendevalda vid behov.

Kommunstyrelsen beslutar om vilken rättighet (behörighet) en förtroendeman ska ha att utnyttja IT-system och den information som finns i det.

## 3.2 Inloggning

Ditt lösenord är strängt personligt och ska hanteras därefter. När du loggar in och arbetar i ett IT-system lämnar du spår efter dig. De loggningsfunktioner som finns i systemen används för att spåra obehörig åtkomst.

Tänk på att du personligen är ansvarig för de aktiviteter som loggas till din behörighet. Du kan själv bli misstänkt om någon använder ditt lösenord för olämpliga ändamål. Du ska därför:

- Aldrig låna ut din behörighet till andra
- Skydda ditt lösenord väl
- Omedelbart byta lösenord om du misstänker att någon känner till det
- Gruppkonton kan förekomma men ska användas restriktivt. Ansvarig person ska alltid finnas utsedd. *(Rutin bör tas fram)*

[1] Internet och gemensam yta för lagring samt e-post.

### 3.2.1 Glömt lösenord till datorn/nätverk

Efter sex misslyckade inloggningsförsök i nätverket kommer ditt användarkonto att spärras. Kontot är sedan spärrat i 20 minuter. Om ditt nätverkskonto eller tillgången till ett specifikt IT-system blir spärrat ska du kontakta IT-supporten.

### 3.2.2 Glömt lösenord till IT-system

Om du glömt ditt lösenord till ett specifikt IT-system ska du kontakta applikationsansvarig för detta system.

## 3.3 Val av lösenord

Du väljer själv nytt lösenord till nätverket. Lösenordet:

- Ska vara minst 6 tecken och max 15 tecken
- Ska innehålla minst en versal, en gemen och en siffra
- Ska vara unikt (aldrig tidigare använt)
- Får inte vara användarens, förnamn, efternamn, för och efternamn
- Får inte innehålla tecken som t ex &%…. (specialtecken)
- Får inte innehålla bokstäverna ÅåÄäÖö

För lösenord i specifika IT-system gäller olika krav. Kontakta respektive systemförvaltare eller IT-avdelningen för mer information.

## 3.4 Byte av lösenord

I datorn ska du byta lösenord fyra gånger per år (var tredje månad). Du får en automatisk påminnelse när det är dags och byter själv lösenordet.

Du kan dessutom själv när som helst byta lösenordet i datorn genom att trycka Ctrl-Alt-Del och välja Ändra lösenord.

För specifika IT-system ska lösenordet bytas efter det tidsintervall som bestämts av applikationsansvarig. I möjligaste mån ska byte av lösenord ske fyra gånger per år.

# 4 Din arbetsplats

## 4.1 IT-utrustning

Den utrustning du förfogar över (som till exempel stationär dator eller bärbar pc, tunn klient, handdator) tillhör Ale kommun.

- Du ska behandla utrustningen varsamt
- Du får inte göra fysiska ingrepp (installationer) på någon utrustning som tillhör Ale kommun.
- Felanmälan av utrustning görs till IT-supporten

Om du behöver ny hårdvara som till exempel USB-minne, tangentbord, mus och liknande ska du kontakta IT-samordnaren.

Inköp av utrustning ska godkännas av din närmaste chef.

## 4.2 Programvaror

När du behöver installera en ny programvara eller konfigurera den (ställa in programmet så att den fungerar på din dator) kontaktar du IT-samordnaren. Det är enbart IT-avdelningen som får installera och konfigurera program på kommunens datorer.

Det är inte tillåtet att kopiera eller använda kommunens program utanför verksamheten.

Innan en ny programvara installeras måste den certifieras för användning i kommunens nätverk. Enbart de programvaror som godkänts i certifieringen får användas på kommunens datorer.

## 4.3 Service på utrustning

Om din mobila enhet (handdator, mobiltelefon) eller annan utrustning som kan innehålla information behöver service som innebär att utrustningen lämnas bort måste all personlig och känslig data (information) som ska sparas först kopieras till din hemkatalog på nätverket och sedan raderas från datorns hårddisk.

Ansvaret ligger på dig som användare men rådgör alltid med IT-samordnaren innan din utrustning lämnas bort!

## 4.4 Kassering av IT-utrustning

Kontakta IT-avdelningen för information om hur omhändertagandet av kasserad utrustning ska ske.

## 4.5 När du tar paus och när du slutar för dagen

Varje gång du lämnar din arbetsplats ska du låsa datorn. Detta gör du med snabbkommandot "CTRL+ALT+DEL" eller med ”Windows tangenten+L” och sedan klicka på Lås arbetsstation. Du låser upp genom att använda samma snabbkommando, och därefter logga in med ditt lösenord.

När du går hem för dagen skall du logga ur alla program och IT-system och sedan stänga av datorn.

### 4.6 Utskrifter av dokument

Det material du skriver ut på en skrivare som har flera användare ska du hämta så snart du kan. Tänk på att kvarglömda dokument kan komma i orätta händer.

Om du ska skriva ut känslig information bör du om det finns möjlighet använda en skrivare med ”tagg” där du får ut ditt material.

### 4.7 Distansarbete och mobil datoranvändning

Du kan nå filer, applikationer och e-post när du sitter utanför din arbetsplats via säker inloggning (fjärrskrivbord). Du får tillgång till denna tjänst efter godkännande av din chef. Beställning sker på samma sätt som beställning av id och systemtillgång, se avsnitt 3.1. Godkänd blankett skickas till IT-avdelningen för utförande.

Följande regler gäller vid uppkoppling via säker inloggning (fjärrskrivbord):

- Datorn du använder ska ha aktuella säkerhetspatchar installerade samt en uppdaterad virusklient
- Var försiktig med utskrifter som sker utanför kommunens lokaler.
- Tänk på att man bara tillfälligt får spara ned dokument eller andra filer på den lokala dator du använder. Dokumentet eller filen måste tas bort efter arbetet.

# 5 Kringutrustning

## 5.1 Allmänt

All IT-utrustning som du förfogar över ska låsas samt lösenordsskyddas. Detta gäller även utrustning som mobiltelefon, handdator. Lösenordsskyddet ska aktiveras efter en minut på mobiltelefoner och handdatorer.

Håll alltid din bärbara utrustning under uppsikt, om du inte har möjlighet att låsa in den.

## 5.2 Bärbara datorer och hemdatorer

En bärbar dator eller hemdator kan innebära vissa säkerhetsrisker. Du bör därför tänka på hur du hanterar denna utrustning.

- Inget sekretessmaterial får lagras på datorns interna hårddisk.
- Du måste alltid se till att datorn är uppdaterad. Detta löser du genom att koppla in datorn i kommunens nät minst varannan vecka. Datorn uppdaterar då antivirusprogrammet och väntande säkerhetsuppdateringar installeras.
- Du får aldrig stänga av antivirusprogrammet på datorn.
- Om du loggar in via bredband hemifrån eller från annan plats ska du använda säker inloggning (fjärrskrivbord).
- Du får inte förvara den bärbara datorn så att du kan förlora densamma (till exempel låta den ligga kvar i bilen). Du förlorar då både datorn och innehållet som finns lagrad på datorn om datorn blir stulen.
- Den information du har på din dator måste skyddas. Se till att alltid ha ett lösenord på inloggningarna som finns på datorn.
- Tänk på att om du endast sparar informationen i den bärbara datorn och datorn stjäls eller går sönder så finns ingen säkerhetskopiering på informationen. Detta löser du genom att se till att kopiera/flytta över informationen till din hemmakatalog (H:) när du är inloggad i Ale kommuns nät.

Om du använder din bärbara PC för hemarbete ska du tänka på att den kan utgöra en säkerhetsrisk och att du inte får lagra sekretessbelagd eller för verksamheten känslig information på den.

Det är ditt personliga ansvar att kontrollera att säkerhetskopiering av informationen fungerar som den ska.

Arbetsrelaterad information/data får inte sparas på en privat dator.

## 5.3 Kringutrustning med mellanlagringsmöjligheter

Handdatorer, mobiltelefoner, USB-minnen och liknande kan lätt bli virusbärare eftersom man kan mellanlagra information i dessa enheter. Tänk på säkerhetsriskerna när du ansluter sådan utrustning till kommunens datorer. Utrustning som inte är godkänd av Ale kommun får ej anslutas till nätverket. Om du är osäker på viken utrustning som får anslutas ska du rådgöra med IT-avdelningen.

Informationen i till exempel handdatorer, digitala kameror, mobiltelefoner, USB-minnen är åtkomligt direkt när du kopplar in det i datorn, vilket gör att informationen kan bli tillgänglig för obehöriga om lagringsmediet kommer i orätta händer. Därför är det inte tillåtet att lagra känslig[2] information på flyttbar lagringsmedia.

[2] Känslig information kan till exempel vara information som omfattas av personuppgiftslagen PUL.

# 6 Klassning, lagring och hantering av information

## 6.1 Lagring

### 6.1.1 Systemdiskar där du kan spara information

Spara alla viktiga dokument på enhet H:\ eftersom backup rutinerna inte omfattar andra enheter såsom t.ex. C:\ och D:\.

Spara dokument på enhet H:\dokument eller i enhet G:\, som kan läsas av alla beroende på behörighet. Sekretessbelagd information får INTE lagras i dessa enheter utan hanteras i respektive verksamhetssystem.

### 6.1.2 Systemdiskar som du inte kan eller inte ska spara information på

C:\ - Lokal systemdisk. Spara inte på C: eftersom det inte finns någon säkerhetskopiering på denna disk. Måste du av någon anledning mellanlagra på denna disk spara i Mina Dokument, så sker en mappsynkronisering när du loggar in i Ale kommun nät.

### 6.1.3 Att spara på bärbar dator

Om du använder någon av Ale kommuns bärbara datorer lagras informationen lokalt på datorn. Information om hur du ska sköta lagring och säkerhetskopiering på en bärbar dator finns i avsnitt 5.2 ”Bärbara datorer och hemdatorer”.

### 6.1.4 Skyddat material

Det är inte tillåtet att lagra eller sprida copyright-skyddat material som till exempel mp3-musik, filmer och liknande.

## 6.2 Klassning och hantering av information

### 6.2.1 Information som hanteras i IT-system

IT-system inom Ale kommun klassas utifrån den information som hanteras i systemet. Klassning görs utifrån sekretess, riktighet, tillgänglighet och spårbarhet.

- **Sekretess:** Information skyddas så den inte avsiktligt eller oavsiktligt görs tillgänglig eller avslöjas för obehörig eller kan nyttjas på annat otillåtet sätt.
- **Riktighet:** Information är skyddad mot oavsiktlig och avsiktlig förvanskning.
- **Tillgänglighet:** Information är tillgänglig för behörig användare, inom eller utanför kommunen

Om du lagrar information på andra media än kommunens gemensamma diskar (till exempel USB-minnen) får det aldrig innehålla konfidentiella eller känsliga uppgifter och det är du själv som är ansvarig för säkerhetskopiering.

### 6.2.2 Information på annan media

Med annan media menas papper, film, DVD, OH-bilder etc.

I de fall ett dokument, av någon typ, betraktas som så känsligt att det inte ska lagras på i nätet ansluten server (högsta säkerhetsklassning) ska särskilt rutin tillämpas. Nedan beskrivs hur den information som lagras på i nätet ansluten server ska klassificeras/hanteras.

Om informationen på sådan media är kopierad ska den hanteras med samma säkerhet som det system som den kommer ifrån. Eftersom informationen är kopierad behöver endast kraven på sekretess (konfidentialitet) beaktas. De krav på sekretess som ställs för ett specifikt IT-system framgår av användarhandledningen för systemet.
Följande krav gäller:

Allmän handling:

- Tillhandahålls allmänheten
  Alla inkomna eller upprättade handlingar som inte är sekretessbelagda.
  Dokumenten är till för alla, det vill säga de får spridas både internt inom Ale kommun och offentligt. Publicerade dokument ska vara skrivskyddade på ett sådant sätt så att ingen förändring kan ske av informationen.

  Viktigt är också att skilja på *allmän handling* och *offentlig handling*: En allmän handling (alltså en handling som är förvarad, samt inkommen till eller upprättad hos myndigheten) behöver inte samtidigt vara offentlig. För att en handling ska vara offentlig krävs
  (1) att den är en allmän handling och
  (2) att den inte är sekretessbelagd.

# 7 Internet

Internet och sociala medier är ett arbetsverktyg och får för privat bruk användas bara i sådan omfattning att det inte inkräktar på arbetet eller medför onödiga kostnader för arbetsgivaren.

När du använder Internet och sociala medier kan säkerheten i kommunens lokala nätverk påverkas i mycket hög grad beroende på ditt beteende. Ale kommun förutsätter att den som surfar på Internet endast besöker välrenommerade webbplatser.

Det är inte tillåtet att för privata syften använda Internet och sociala medier för att titta eller lyssna på material av pornografisk, rasistisk karaktär, eller extrempolitiskt innehåll. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning, och liknande) eller har anknytning till kriminell verksamhet.

I specifika fall kan det dock vara motiverat för arbetet, till exempel vid utredningar, omvärldsanalyser med mera, att besöka sidor som normalt är förbjudna. Beslut om detta ska fattas av närmaste chef.

När du surfar på internet representerar du Ale kommun. Följ därför noga kommunens riktlinjer och policys. Du lämnar alltid spår efter dig på Internet i form av kommunens IP-adress.

# 8 E-post

Tillgången till minne för e-post är begränsad. E-postsystemet ska därför inte användas som ett arkiv. Tänk på att regelbundet radera i mapparna ”Inkorgen”, ”Skickat”, och ”Borttaget” för att frigöra utrymme. Om du har för mycket material i e-postprogrammet får du automatisk ett meddelande om att radera. Glömmer du att göra det kan din e-post spärras.

Meddelanden och bifogade filer som du vill spara hanterar du på samma sätt som du hanterar annan information (se kapitel 6).

När du använder e-post gäller följande:

- Sekretessbelagd eller integritetskänslig information får inte skickas via e-post.
- Är du borta från jobbet ska du aktivera frånvarobeskedet och ange vem som tar hand om dina inkommande ärenden under tiden du är borta.
- Om du får en bifogad fil ska du öppna den enbart om du känner till och litar på avsändaren.
- Misstänker du att du fått virus i e-posten ska du kontakta IT-avdelningen (se vidare i kapitel 9).
- E-post är ett arbetsverktyg och får för privat bruk användas bara i sådan omfattning att det inte inkräktar på arbetet eller medför onödiga kostnader för arbetsgivaren.
- Det är inte tillåtet att automatiskt vidarebefordra all inkommande e-post till annan e-postadress utanför Ale kommun.
- Kontrollera vilka som är medlemmar på sändlistor innan du använder dem. Det finns risk att känslig information annars når fel mottagare.
- E-post ska diarieföras enligt samma regler som vanlig post.

## 8.1 Webmail

Du kan nå din e-post via vilken dator som helst som har en Internetuppkoppling.

Se avsnitt 3.2 angående lösenords hantering.

# 9 Incidenter

En IT-incident är en oönskad, negativ händelse för kommunens information och IT-system, som till exempel att informationen inte är tillgänglig, har tagits bort eller förvanskats. En IT-incident påverkar eller kan komma att påverka kommunen negativt när det gäller sekretess, tillgänglighet och riktighet.

Exempel på IT-incident kan vara:

- Att tjänster, funktioner, utrustning eller andra resurser inte fungerar som de ska.
- Systemfel eller överbelastning
- Misstag
- Försummelse när det gäller att följa policies eller rutiner.
- Någon har tagit sig in i system som man inte har behörighet till.

En IT-incident kan uppstå genom att exempelvis:

- Obehöriga får tillgång till kommunens information (sekretess)
- Kommunens IT-system är inte tillgängliga på avsett vis (tillgänglighet)
- Kommunens information är oriktig, förvanskad eller ofullständig (riktighet)

Om du misstänker att någon har använt din identitet eller att någon obehörig varit inne i kommunens system ska du:

- Notera när du senast var inne i IT-systemet.
- Notera när du upptäckte händelsen.
- Omedelbart anmäla detta till IT-avdelningen eller till din närmaste chef.
- Dokumentera alla iakttagelser i samband med upptäckten och försöka ta reda på om kvaliteten på din information har påverkats

Om du misstänker stöld, brand, sabotage eller liknande ska du kontakta din närmaste chef.

Om du upptäcker fel och brister i de system du använder ska du rapportera dessa till IT-avdelningen.

# 10 Skadlig kod (virus med mera)

Skadlig kod är små program som laddas ner i din dator utan din vetskap och ditt samtycke. Dessa kan göra allt ifrån att bara visa ett meddelande till att kontrollera vad som görs på datorn eller ge utomstående användare tillgång till vårt nätverk. Svåra utbrott av datavirus kan leda till att kommunens hela nätverk slutar fungera. Gratisprogram, spelprogram och filer som laddas ned från Internet eller filer som bifogas till e-post är de vanligaste smittbärarna.

Tecken på datavirus i systemet kan vara att:

- Virusprogrammet varnar att den upptäckt ett virus.
- Datorn gör saker utan att man själv har satt igång det, till exempel att filer försvinner eller ändras och att program startar.
- Datorn arbetar mycket långsamt.

Om du misstänker att datorn innehåller virus eller liknande ska du:

- Dra ut nätverkskabeln, men låta datorn vara på.
- Omedelbart anmäla detta till IT-avdelningen. Observera att anmälan ska göras per telefon eller besök, *inte* per e-post.

Om du får brev med virusvarning där man talar om att ett virus är på gång ska du inte skicka meddelande om detta till alla på arbetsplatsen. Kontakta istället IT-avdelningen som kan avgöra om det är en seriös varning eller inte.

# 11 När du slutar jobba i Ale kommun

När du avslutar din anställning ska du:

- Lämna tillbaka all utrustning som tillhör Ale kommun till din närmaste chef.
- Rådgöra med din chef om vilket av ditt arbetsmaterial som ska sparas. Notera att allt material du framställt i samband med din tjänst är Ale kommuns egendom och inte får tas med utan din chefs godkännande.
- Vidarebefordra information och dokument till lämplig person efter samråd med din chef.

De behörigheter du fått till Ale kommuns datasystem avbeställs av närmaste chef.