Österåker

Österåkers kommuns styrdokument
Datum för antagande: 2026-xx-xx
Diarienummer: KS 2026/0215
Antagen av:
Dokumentansvarig: Kommunstyrelsens förvaltning

Riktlinjer för AI-användning i Österåkers kommun



POLICY • PROGRAM • STRATEGI • HANDLINGSPLAN • RIKTLINJE

Innehåll

Inledning 3
Syfte 3
Vilka som berörs 3
Riktlinjens koppling till andra styrdokument 3
Kommunikation 3
Aktualitetsprövning och revidering 4
Vilka möjligheter skapar AI? 5
Vilka riskfaktorer bör beaktas? 5
Vad har jag för ansvar som medarbetare? 6
Förtroende och transparens 6
Informationssäkerhet och dataskydd 7
Transkriptioner i Teams 8
Vad är viktigt att tänka på vid AI-användning? 9
Microsoft Copilot 10
Google Gemini och Notebook (avser enbart UBF) 10
Övriga AI 10
Användning av generativ (skapande) AI 11
Användning av AI-genererade bilder 11
Immateriella rättigheter 11
Vad bör jag tänka på vid anskaffning och tillämpning av egna lösningar? 12
Hur begränsar jag klimatpåverkan från AI-användning? 14
Hur rapporterar jag en incident? 15
Bilaga A: Centrala begrepp 16
Bilaga B: Matris för informationshantering 18

Inledning

Artificiell intelligens, AI, skapar nya möjligheter för Österåkers kommun att utveckla verksamheten, förbättra service till invånare och effektivisera arbetssätt. Samtidigt innebär användningen av AI ett ansvar, både juridiskt, etiskt och verksamhetsmässigt. För att stärka förtroendet för kommunen behöver vi vara öppna, noggranna och medvetna om både nyttan och riskerna.

Dessa riktlinjer ger ett gemensamt ramverk för hur AI ska användas i kommunens verksamheter. De ska stödja dig som medarbetare att använda AI på ett säkert, ansvarsfullt och ändamålsenligt sätt.

Genom att förena innovation med fokus på informationssäkerhet, dataskydd och god förvaltning kan kommunen använda AI på ett hållbart sätt till nytta för både verksamheten och invånarna.

Syfte

Syftet med riktlinjerna är att ge dig som medarbetare tydligt stöd för hur AI ska användas säkert och ansvarsfullt. Riktlinjerna ska också göra det lättare för dig att känna dig trygg i hur du kan använda AI i arbetet. Dokumentet ska hjälpa kommunen att följa EU:s AI-förordning och GDPR, och tydliggör att du har ett personligt ansvar när du använder både publika och upphandlade AI-tjänster.

Vilka som berörs

Riktlinjerna gäller alla anställda i Österåkers kommun. De gäller också konsulter, inhyrd personal och leverantörer som hanterar kommunens information.

Riktlinjens koppling till andra styrdokument

Riktlinjerna förtydligar kommunens AI-policy, informationssäkerhetspolicyn och stödjer kommunens mål i budgeten om effektivisering och modern service. De kopplar också till lagar och regler som kommunen måste följa, till exempel EU:s AI-förordning, GDPR, cybersäkerhetslagen, kommunallagen, offentlighets- och sekretesslagen (OSL) samt förvaltningslagen.

Kommunikation

Riktlinjerna publiceras på kommunens intranät och sprids via ledningssystemet till alla förvaltningar. Informationen ska också ingå i obligatoriska utbildningar.

Gemensamma utbildningsinsatser tas fram centralt och utgår från kommunens AI-policy och dessa riktlinjer. De syftar till att ge alla medarbetare en enhetlig grundläggande förståelse för AI, relevanta lagkrav samt hur riktlinjerna ska tillämpas i praktiken.

Respektive förvaltning ansvarar därutöver för att identifiera sina egna behov och ta fram verksamhetsanpassade rutiner, anvisningar samt utbildningar. Dessa ska utgå från den egna verksamhetens förutsättningar, risker och användningsområden, och bidra till att stärka medarbetarnas förmåga att använda AI på ett säkert och ändamålsenligt sätt i det dagliga arbetet.

Kompetensen behöver utvecklas löpande i takt med att tekniken och regelverken förändras. Därför ska utbildningsinsatser följas upp och uppdateras regelbundet, samt kompletteras med stöd och vägledningar vid behov.

Aktualitetsprövning och revidering

Eftersom AI och lagstiftning utvecklas snabbt ska riktlinjerna ses över årligen. Dokumentet ska även uppdateras vid större förändringar i EU-regelverk eller när nya nationella vägledningar tillkommer. Därutöver ska riktlinjerna revideras vid behov, exempelvis vid identifierade risker eller incidenter i verksamheten. Revideringen initieras och genomförs av kommunstyrelsens förvaltning (KSF).

Österåker

Vilka möjligheter skapar AI?

AI kan ge stor nytta och du uppmuntras att utveckla arbetssätt med hjälp av ny teknik. Samtidigt behöver användningen vara genomtänkt och ansvarsfull.

Med AI kan du till exempel:

- **Automatisera rutinuppgifter** så att du frigör tid till viktigare uppgifter.
- **Effektivisera processer** genom att hitta onödiga steg och förbättra arbetsflöden, eller skapa verktyg som underlättar arbetsprocesser.
- **Söka och sammanställa information** snabbare, även i stora mängder material.
- **Få stöd för text och bild**, till exempel förslag på formuleringar, översättning eller bildgenerering.
- **Göra analyser av data** för att se mönster, få underlag och stödja beslut.
- **Öka tillgänglighet**, till exempel genom snabbare svar och kortare väntetider – om AI används på rätt sätt.

Vilka riskfaktorer bör beaktas?

AI innebär stora möjligheter, men det finns också risker. Om du använder AI utan att tänka efter kan det få negativa konsekvenser. AI kan gradvis skapa ett undermedvetet förtroende som gör att vi ifrågasätter svaren mindre. Var därför medveten om detta och säkerställ att du alltid gör en egen kritisk bedömning av innehållet. Var särskilt uppmärksam på:

- **Fördomar (bias):** AI tränas på data som kan innehålla snedvridningar. Det kan leda till orättvisa eller diskriminerande resultat, särskilt i känsliga frågor.
- **Insamling av persondata:** vissa tjänster samlar in mycket information om användare. Om data läcker eller missbrukas kan det få allvarliga följder.
- **Polarisering och desinformation:** AI kan användas för att skapa och sprida falsk information, till exempel så kallade deepfakes.
- **Felaktiga svar:** AI kan ge svar som låter rimliga men som egentligen är felaktiga eller påhittade. Du måste alltid kontrollera fakta.
- **Brist på förståelse:** AI räknar sannolikheter och förstår inte sammanhang som människor gör. Den kan därför ge olämpliga eller skadliga svar.

Vad har jag för ansvar som medarbetare?

AI kan hjälpa dig att komma igång och arbeta mer effektivt, men du måste alltid använda ditt eget omdöme. Det är i slutändan du som står för innehållet och konsekvenserna.

Krav:

- Du får inte låta AI ta över yrkesmässiga bedömningar eller beslut i myndighetsutövning.
- Du ska vara medveten om att du är personligt ansvarig för all information du matar in i AI, och för hur du använder resultatet.
- AI-genererat material ska alltid ses som ett utkast och får inte användas utan att du som medarbetare granskar det kritiskt, eftersom AI kan hitta på och presentera fel som sanning.

Förtroende och transparens

Offentlig sektor bygger på högt förtroende. Därför behöver AI användas på ett sätt som är tydligt, lagligt och möjligt att följa upp. I Sverige finns rätt till insyn, vilket innebär att handlingar ska diarieföras eller hållas ordnade så att de kan lämnas ut. Därför behöver verksamheten tänka på om AI-användning skapar nya allmänna handlingar – och hur de i så fall ska sparas och diarieföras.

Enligt förvaltningslagen ska kommunen kunna motivera beslut. Om AI används på sätt som påverkar invånare behöver det finnas en förståelse för att kunna beskriva hur AI bidragit. Samtidigt kan vissa AI vara svåra att förklara i detalj. I vissa sammanhang kan det därför vara olämpligt att använda AI.

Krav:

- Om AI har använts för att skapa eller väsentligt bearbeta material som kommuniceras externt ska detta anges om det efterfrågas eller är viktigt för mottagarens förtroende. Se separat avsnitt gällande AI-genererade bilder.
- Om AI används på ett sätt som påverkar invånare ska verksamheten kunna beskriva hur AI har använts och hur det har hjälpt till i bedömningen eller beslutet.
- Du ska dokumentera och diarieföra allmänna handlingar som skapas med stöd av AI enligt offentlighetsprincipen.

Informationssäkerhet och dataskydd

Använder du Copilot i inloggat läge (eller Gemini för utbildningsförvaltningen) så används inte din data för träning. Använder du någon annan AI behöver du veta hur leverantören kan använda den information eller det material du infogar. Ta reda på om leverantören garanterar att det som matas in inte används för träning eller om det finns risk att det du infogar kan dyka upp i svar till andra. Om information återanvänds kan den i praktiken spridas öppet.

Det är varje förvaltnings ansvar att avgöra vilken informationsklass som gäller för sina system. AI får bara användas om det är godkänt för just den informationen.

Det finns också information som inte är sekretess, men ändå kan vara känslig om den hamnar fel, till exempel innehåll från interna möten eller preliminära bedömningar i ärenden.

Krav:

- Du får aldrig ge AI åtkomst till information på din enhet, som kontakter eller filer, utan godkännande från Digitaliseringsavdelningen.
- Det är strängt förbjudet att mata in sekretessbelagd information, personnummer eller känsliga personuppgifter i allmänt tillgängliga AI-tjänster (som gratisversionen av ChatGPT).
- All information som hanteras i AI-system ska vara klassificerad och systemet ska vara godkänt för den aktuella informationsklassen.
- Innan personuppgifter behandlas i ett nytt AI-system ska en tröskelanalys och vid behov en konsekvensbedömning (DPIA) göras i samråd med dataskyddsombudet. Digitaliseringsavdelningen kan bistå med metoder för anonymisering.

Kontakta informationssäkerhetssamordnare på respektive förvaltning vid frågor om informationssäkerhet. Och i andra hand informationssäkerhetsansvarig på avdelningen för säkerhet, trygghet och civil beredskap. Vid frågor om personuppgifter: kontakta dataskyddsombudet (DSO) på Kommunkansliet.

Transkriptioner i Teams

AI-transkription i Teams är ett kraftfullt stöd för dokumentation och tillgänglighet men ska användas med eftertanke och i linje med kraven på informationssäkerhet. När du använder AI-baserad transkription är det viktigt att vara medveten om följande:

- **Innehållet kan bli känsligt**
  Allt som sägs dokumenteras. Undvik att dela sekretessbelagd, personkänslig eller säkerhetsklassad information i möten där transkription är aktiverad.
- **Behörigheter och åtkomst**
  Säkerställ att endast rätt personer har tillgång till transkriptionen. Kontrollera delning och lagringsinställningar.
- **Informera deltagare**
  Deltagare ska veta att mötet transkriberas. Transparens är viktigt både juridiskt och etiskt.
- **Lagringstid**
  Följ organisationens riktlinjer för hur länge transkriptioner får sparas och när de ska tas bort.
- **AI är ett stöd – inte ett facit**
  Transkriptioner kan innehålla fel. De ska inte användas som enda källa vid känsliga beslut.

Vad är viktigt att tänka på vid AI-användning?

Oavsett vilken AI du använder gäller följande:

- Du är alltid ansvarig för att materialet är faktamässigt korrekt, har professionell tonalitet och är fri från fördomar och annan bias.
- Du kan inte överlåta din yrkesmässiga bedömning till en generativ AI.
- Du ansvarar för materialet som om du själv hade skapat det.
- Var transparent med användningen av generativ AI om du har använt hela eller delar av din text, bild eller annat genererat material, särskilt om mottagaren efterfrågar det. Detta gäller både i externa och interna sammanhang.

Krav:

- För arbete med intern eller känslig information ska du alltid använda kommunens upphandlade tjänster* (till exempel Microsoft Copilot) och vara inloggad med ditt tjänstekonto.
- Vid användning av Copilot ska du kontrollera att den gröna sköldikonen visas (uppe i högra hörnet i verktyget), som ett tecken på att företagsdataskydd är påslaget och att data inte används för att träna modellen.
- Allmänt tillgängliga AI-tjänster får bara användas för information som redan är offentlig och som skulle kunna publiceras på kommunens webbplats.

* Information om upphandlade system återfinns på Inomskärs, under ”Verksamhetssystem”.

Microsoft Copilot

Copilot finns i kommunens M365-miljö. När du använder Copilot inloggad med ditt Österåker-konto hanteras informationen i Microsofts moln på samma sätt som annan information i M365 (till exempel OneDrive och Outlook). Även då får känsliga personuppgifter, särskilt skyddsvärda personuppgifter och sekretessbelagda uppgifter inte behandlas i Copilot.

När du är inloggad med kommunens konto ska du se en **grön sköld**. Om du inte är inloggad gäller reglerna för allmänt tillgängliga AI-system.

Google Gemini och Notebook (avser enbart UBF)

Gemini och Notebook ingår som kärntjänster i kommunens avtal med Google vilket innebär att när du är inloggad med ditt Workspace for Education konto används inte data för att träna AI språkmodellen. Avtalet gäller enbart för pedagoger och elever i kommunala förskolor och skolor.

Även som inloggad får känsliga personuppgifter, särskilt skyddsvärda personuppgifter och sekretessbelagda uppgifter inte behandlas i Gemini eller Notebook.

När du är inloggad med kommunens konto ska du se det i cirkeln högst upp till höger. Om du inte är inloggad gäller reglerna för allmänt tillgängliga AI-system.

Övriga AI

ChatGPT är inte informationsklassat eller konsekvensbedömt. Därför gäller reglerna för allmänt tillgängliga AI-system oavsett om du använder gratisversion, privat betalversion eller får åtkomst via arbetet.

Samma gäller för andra typer av AI, exempelvis Grok, Claude, Perplexity med flera.

Användning av generativ (skapande) AI

Generativ AI kan skapa nytt innehåll utifrån dina instruktioner. Du ansvarar alltid för resultatet och måste därför kontrollera det.

Kom ihåg: generativa AI är inte sökmotorer. De kan skapa material som ser trovärdigt ut, men det betyder inte att det är korrekt, lämpligt i ton eller fritt från bias (fördomar/partiskhet). AI kan ge olika svar på samma fråga och kan bygga på källor som inte är pålitliga.

Behandla därför alltid AI-resultat som ett utkast. Du kan inte lämna över din yrkesbedömning till AI, och du ansvarar för materialet som om du själv skrivit det. Var också öppen med AI-användning när det är relevant eller när någon frågar.

Användning av AI-genererade bilder

Internt: AI-genererade bilder och infografik får användas för interna ändamål, exempelvis i undervisning, utbildning, arbetsmöten eller för att illustrera möjliga framtida utvecklingar. Om bilderna används i sammanhang där verksamheten representeras eller vid större möten och presentationer ska de vara förenliga med kommunens riktlinjer för grafisk profilering. Exempel på större möten är chefsforum, förvaltningsmöten och inomskärsmöten. För att värna transparens och trovärdighet ska det alltid framgå när AI-genererade bilder används.

Externt: Samtlig extern kommunikation ska alltid vara förenlig med kommunens riktlinjer för grafisk profilering, där användning av AI-genererade bilder som regel är uteslutet.

Se kommunens riktlinjer för grafisk profilering för ytterligare instruktioner om bildanvändning.

Immateriella rättigheter

Immaterialrätt handlar om ensamrätt till skapelser, till exempel upphovsrätt och patent. Intrång kan ske både när du matar in material och när AI skapar resultat. Tänk särskilt på detta vid generativ AI. Det är bra att veta att lagar, domar och myndighetsbeslut normalt inte omfattas av upphovsrätt.

Krav:

- Du ska säkerställa att du inte matar in upphovsrättsskyddat material i AI på ett sätt som bryter mot licensvillkor.
- Du ska vara uppmärksam på att AI-genererat material kan likna befintliga verk, vilket kan innebära risk för upphovsrättsintrång vid publicering.

Vad bör jag tänka på vid anskaffning och tillämpning av egna lösningar?

Att köpa in eller utveckla olika typer av AI ska ingå i kommunens ordinarie styrning och utvecklingsarbete. När kommunen anskaffar eller utvecklar egen AI ska det bedömas hur systemet och leverantören skyddar information. Det behöver också ställas krav i avtal, funktioner och arbetssätt så att kommunen behåller kontroll över data och kan följa lagar.

Det är viktigt att AI-systemet är tillräckligt transparent och uppfyller krav utifrån gällande regler (till exempel OSL, GDPR, förvaltningslagen, kommunallagen och EU:s AI-förordning).

Så kallad högrisk-AI, inom till exempel utbildning, rekrytering och myndighetsutövning, har extra höga krav. Därför behöver kommunen tidigt avgöra om ett planerat användningsområde är högrisk. Om kommunen använder ett högrisksystem i verksamheten kan kommunen få rollen som tillhandahållare enligt AI-förordningen, vilket innebär fler krav på dokumentation, kontroll och uppföljning. Om kommunen själv utvecklar högrisk-AI kan kraven bli ännu högre.

Vid inköp av högrisk-AI behöver särskilda krav ställas på leverantören. Vid utvecklingssamarbeten behöver det vara tydligt att någon annan än kommunen tar rollen som leverantör enligt AI-förordningen.

Vid anskaffning hänvisas medarbetare till Digitaliseringsavdelningens avsnitt om Businesscase på Inomskärs.

Krav:

- Kommunen ska inte agera som leverantör av egna högrisksystem, eftersom resurser för certifiering och teknisk dokumentation saknas

- Vid anskaffning av AI-system ska en riskbedömning göras tidigt för att se om systemet klassas som högrisk enligt EU:s AI-förordning.

- Vid experimentell utveckling (till exempel i Power Platform) får inga verkliga personuppgifter eller sekretessbelagd information användas, såvida inte en valideringsmetod tillämpas som säkerställer

Hur begränsar jag klimatpåverkan från AI-användning?

AI använder energi och påverkar klimatet. Därför ska AI användas med eftertanke och bara när det ger tydlig nytta i arbetet. När du använder AI, försök att:

- **Tänka före:** använd AI när det sparar tid eller ersätter ett krävande moment.
- **Ställa genomtänkta frågor:** bra och samlade frågor minskar beräkningar.
- **Undvika upprepningar:** ställ inte samma fråga flera gånger i onödan.
- **Välja enklare lösningar när de räcker:** mallar och enklare verktyg kan vara nog.
- **Inte skapa onödigt mycket innehåll:** generera inte långa texter/bilder som inte används.
- **Prioritera verksamhetsnytta:** använd AI för att förbättra kvalitet, spara tid eller stödja beslut – inte för privata ändamål.
- **Starta ny chatt ofta:** Allt som står i ditt chattfönster skickas med i varje prompt, så en lång tråd kräver mer prestanda än en kort.
- **Klistra enbart in den kontext som modellen behöver:** Till exempel om ett beslut gäller tre punkter – skicka tre punkter. Det ger bättre och billigare svar.
- **Matcha modell mot uppgift:** du behöver inte bästa modellen till allt. Enkla modeller räcker ofta för text – spara de tyngsta modellerna till analys, kod och komplexa avvägningar.

Hur rapporterar jag en incident?

Om eller när AI skapar innehåll som bedöms kunna orsaka skada ska detta alltid rapporteras till närmsta chef. Med skadligt innehåll menas sådant som på något vis kan orsaka fysisk, psykisk, juridisk, ekonomisk eller organisatorisk skada.

Kommunens rutin för hantering av personuppgiftsincidenter.

Krav:

- Om du upptäcker att känslig information läckt till AI, eller om verktyget skapar skadligt innehåll, ska detta omedelbart rapporteras till närmsta chef. Om informationen innehåller personuppgifter ska även en personuppgiftsincident anmälas.

Bilaga A: Centrala begrepp

Term	Enkel definition
AI (Artificiell intelligens)	Digitala system som kan analysera information, dra slutsatser eller skapa innehåll på sätt som liknar mänsklig bedömning.
AI system	En AI tjänst eller en AI lösning som används för att ta fram resultat, t.ex. text, analys eller underlag.
AI tjänst / AI verktyg	En app eller tjänst med AI funktioner (t.ex. chattbot eller digital assistent).
Allmän handling	Dokument/information som kan behöva lämnas ut enligt offentlighetsprincipen. Om den skapas med AI kan den behöva sparas och diarieföras.
Allmänt tillgänglig AI tjänst (publik AI)	AI tjänst som är öppen för allmänheten. Får bara användas för information som redan är öppen och kan publiceras offentligt.
Annan känslig information	Information som inte måste vara sekretess, men som kan skada individer eller kommunen om den sprids (t.ex. interna möten eller preliminära bedömningar).
Bias (snedvridning/fördomar)	När AI ger svar som blir orättvisa eller snedvridna eftersom den tränats på data med fördomar.
Deepfake	Manipulerat ljud/bild/video som ser äkta ut men är falskt (kan användas för desinformation).
Diarieföra	Att registrera och hantera handlingar så att de är ordnade och går att ta fram vid begäran.
DPIA (konsekvensbedömning)	En analys som görs innan personuppgifter behandlas i ett nytt system, för att bedöma risker och skyddsåtgärder. Ska göras vid behov tillsammans med DSO.
DSO (Dataskyddsombud)	Kommunens stöd i frågor om personuppgifter och dataskydd (GDPR).
Företagsdataskydd (”grön sköld” i Copilot)	Visar att du är inloggad med kommunens konto och att skydd för arbetsdata är aktivt i Copilot.
Generativ AI (skapande AI)	AI som kan skapa nytt material utifrån instruktioner, t.ex. ny text eller bilder.

Term	Enkel definition
Hallucinera	När AI hittar på felaktiga uppgifter som kan låta trovärdiga.
Immaterialrätt/upphovsrätt	Regler om ensamrätt till skapelser (t.ex. texter, bilder). Du måste undvika att mata in eller publicera material så att du gör intrång.
Informationsklass	Den nivå informationen får efter klassning. AI systemet måste vara godkänt för den nivån.
Informationsklassning	Att bedöma vilken "känslighetsnivå" information har (t.ex. öppen, intern, skyddsvärd/sekretess) så att rätt verktyg används. (Generell förklaring – ordet används i dokumentet.)
Krav	Ett obligatoriskt krav som ska uppfyllas, men där det i vissa fall kan finnas utrymme för avsteg om de hanteras formellt och motiveras.
Känsliga personuppgifter	Extra skyddsvärda personuppgifter enligt GDPR (t.ex. hälsa). Sådana får inte matas in i publika AI tjänster och ska hanteras med mycket stor försiktighet. (Generell förklaring – förbudet framgår.)
Myndighetsutövning	När kommunen fattar beslut som påverkar individers rättigheter/skyldigheter. Sådana beslut får inte lämnas över helt till AI.
Sekretessbelagd information	Uppgifter som omfattas av sekretess enligt lag (t.ex. OSL). Får inte matas in i allmänt tillgängliga AI tjänster.
Språkmodell	Den "motor" som genererar text. Den förutspår nästa ord utifrån sannolikhet – inte utifrån vad som är sant.
Tröskelanalys	En första kontroll som hjälper avgöra om en DPIA behövs innan personuppgifter behandlas i ett nytt AI system.
Upphandlad/anpassad AI tjänst	AI tjänst som kommunen har avtalat om eller godkänt. Ska användas för intern eller känslig information enligt riktlinjerna.

Österåker

Bilaga B: Matris för informationshantering

Konfidentialitets-nivåer (0-3) och informationsklasser	**0, Öppen information**	**1, Öppen intern information (ej känslig)**	**2, Begränsad intern information (känslig)**	**3, Sekretess, säkerhetsskydd och känsliga personuppgifter**
Påverkan om informationen skulle spridas	Ingen	Försumbar	Betydande	Allvarlig
Beskrivning	Information som är öppen eller offentlig och kan spridas externt	Information som kan spridas fritt internt inom organisationen	Information som bara ska spridas till de som behöver ta del av den internt och med samarbetspartners	Information som kräver särskild hantering och varsamhet
Exempel	- Kontaktuppgifter till verksamheter - Politiska beslut och styrdokument - Externa nyheter och marknadsföring - Gällande detaljplaner	- Kontaktuppgifter och organisatorisk tillhörighet avseende medarbetare -Verksamhetsplanering - Styrdokument så som riktlinjer, instruktioner, checklistor m.m - Information från intranätet	- Extra skyddsvärda personuppgifter - Namn på barn och elever - Handläggning i enskilda ärenden - Pågående verksamhetsutredningar - Beslutsunderlag och mötesanteckningar	- Handlingar som omfattas av sekretess enligt OSL - Känsliga personuppgifter - Vårdplaner - Juridiska tvister och klagomålsärenden - Omfattande data för forskning från verksamhet - Säkerhetsåtgärder inom IT och fastighet - Sårbarheter och brister inom IT och beredskap
Godkända verktyg och plattformar	- Kommunens webbplatser och sociala plattformar - Allmänna och kommunens egna AI-tjänster - Microsofts verktyg - Googles verktyg	- Intranät och andra interna plattformar - Kommunens egna AI-tjänster - Microsofts verktyg - Googles verktyg	- Godkända kommunikationstjänster för skyddad kommunikation - Lärplattform t.ex. Unikum - Kommunens egna AI-tjänster* (*Det krävs noggrant förarbete och godkännande innan information får hanteras i en AI-tjänst)	- Godkända kommunikationstjänster för skyddad kommunikation - Ej tillåtet att hantera i AI-tjänster.