Ada_Guest_WiFi
surfa2024

Implementering av informations- och kommunikationsteknik

IKT-strategi för undervisningssektorn på Åland 2023 – 2025

Åbo Akademi
Centret för livslångt lärande

John Henriksson – Mia Skog – Roland Träskelin

Program 29.10.2024

09:00 Välkomna

09:10 Trygga elever och lärare, dataskydd – Rolle Träskelin

10:15 Paus

10:30 Miljö och välbefinnande i digitala miljöer – Mia Skog

12:00 Lunch

13:00 Test och diskussion om Escape Room

14:30 Paus

14:45 Gruppdiskussion i blandade grupper

15:30 Sammanfattning

16:00 Avslut

bit.ly/IKTaland

Materialet hittas här

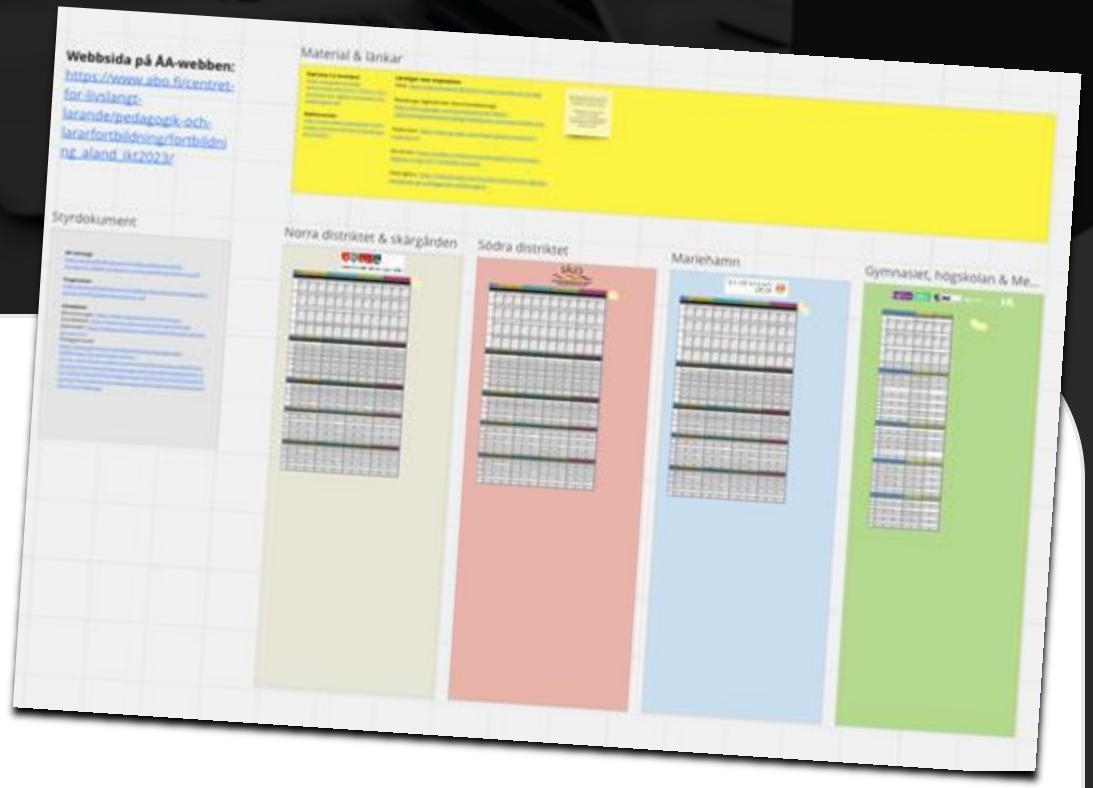
Vår 2024		Höst 2024		
Information och datakunnighet Ledare 31.1 Personal 1.2 Gemensam distansträff Stadiespecifika distansträffar Filmer: Digital lärstig Informations-sökning	**Kommunikation och samarbete** Personal 26.3 Gemensam distansträff Stadiespecifika distansträffar Filmer: Lärarens hantverk Delning av material	Semester	**Skapa digitalt innehåll** Ledare 9.9 Personal 10.9 Gemensam distansträff Stadiespecifika distansträffar 2 filmer	**Säkerhet** Personal 29.10 Gemensam distansträff Stadiespecifika distansträffar 2 filmer	**Problemlösning** Ledare 10.12 Personal 11.12 Gemensam distansträff Stadiespecifika distansträffar 2 filmer

Målsättning: Stöda implementeringen av IKT-strategi för digital kompetens inom utbildningssektorn på Åland 2023–2027.

Progression, struktur & koppling till styrdokument

Personalens kompetens

Verktyg för ledning & implementering



miro

- Gemensamt botten på Miro: https://miro.com/app/board/uXjVNpGbVII=/?share_link_id=386797494362
- Lösen: iktaland
- Bara en gemensam arbetstyta. Det slutliga formatet växer fram under året.
- Ni äger produkten


Here's what she had to say.

Åbo Akademi
Centret för
livslångt lärande

Vilken är föräldrarnas uppgift?

Vilken är bildningens uppgift?

Läroanstalters behov av informations- och kommunikationsteknik

1. Pedagogiska behov

Kan anses omfatta alla tjänster och program som används som stöd i undervisningen under lektionerna och för kommunikation under eventuella distansperioder. Sådana digitala verktyg är grundläggande program, program som olika läroämnen och studieområden behöver, lärandeplattformar samt redskap för distansjobb (videokonferenser osv.). Utöver programvaror är det allt vanligare att använda olika mobila enheter som hjälp på alla skolstadier. Metoderna för fjärradministration av dessa enheter är viktiga med tanke på informationssäkerheten.

2. Studentadministrativa behov

Omfattar grundläggande programverktyg samt system och program för student- och elevadministration och system för elevurval.

3. Anordnaradministrativa behov

Stora utbildningsanordnare har i sin dataadministration egna centrala system som möjliggör tillgång till gemensam information genom en inloggning. Sådana system kan vara exempelvis tjänster för reseadministration eller ekonomiförvaltning som är gemensamma för alla förvaltningsområden.

Hantering och skydd av personuppgifter inom utbildning

En betydande del av den information som hanteras i skolor och läroanstalter är personuppgifter. **EU:s allmänna dataskyddsförordning** (General Data Protection Regulation, GDPR) tillämpas i alla EU-länder från och med 25.5.2018. En person är enligt dataskyddsförordningen identifierbar om hen direkt eller indirekt kan identifieras utgående från personuppgifterna.

Elevernas och studerandenas personuppgifter ska skyddas så att utomstående inte har åtkomst till dem. Med utomstående avser man här även sådan personal vid skolan som inte behöver uppgifterna i sitt arbete. Informationen ska skyddas mot olaga hantering så att den inte av misstag eller olovligt kan raderas, ändras, överlåtas eller flyttas. Dataskyddskraven är särskilt viktiga när det gäller sekretessbelagd eller känslig information.

Handlingar ska förvaras omsorgsfullt. Handlingarna ska förvaras i låsta skåp och datasystemen ska skyddas med användarnamn och lösenord. Skolans personal ges de användarrättigheter som deras respektive arbetsuppgifter kräver och användarrättigheterna övervakas regelbundet. Därtill ska personalen informeras om vikten av dataskydd.

Utbildningsanordnaren eller annan huvudman för läroanstalten är personuppgiftsansvarig vid läroanstalten och säkerställer att personuppgifterna alltid hanteras lagenligt. Inom grundläggande utbildning som kommunen anordnar är kommunens organ med ansvar för undervisningsväsendets administration personuppgiftsansvarig och oftast är det här en nämnd.

DATAINSPEKTIONEN ÅLAND

https://www.di.ax

Dataskyddslagen för Ålands offentliga sektor (landskapslagen om dataskydd inom landskaps- och kommunalförvaltningen ÅFS 2019:9) är ett komplement till EU:s allmänna dataskyddsförordning 2016/679 (dataskyddsförordningen, GDPR). Dataskyddsförordningen är utan komplementet direkt tillämplig lag på Åland.

I lagstiftningshierarkin står EU-förordningar, således dataskyddsförordningen, högst, högre än grundlagen och högre än självstyrelselagen.

https://www.utbildning.ax/digital-kompetens/digitalt-sjalvforsvar

DATASKYDD

CENTRALA BEGREPP

Allmänt

- Dataskydd
- GDPR
- Informations-säkerhet

Kategorisering av data

- Personuppgifter
- Sekretess-belagd uppgift
- Särskilda kategorier av personuppgifter
- Pseudonymi-serade uppgifter
- Offentlig uppgift
- Anonyma uppgifter

Personer och aktörer

- Dataskydds-ombud
- Registrerad
- Personuppgifts-ansvarig
- Gemensam personuppgifts-ansvarig
- Personuppgifts-biträde

Skyldigheter

- Dataskydds-principer
- Personregister
- Grund för behandling
- Den registrerades uppgifter
- Personuppgifts-incident
- Berätta om behandlingen för den registrerade
- Konsekvens-bedömning
- Inbyggt dataskydd och dataskydd som standard

OPETUSHALLITUS
UTBILDNINGSSTYRELSEN

DATASKYDD

CENTRALA BEGREPP

Allmänt

Dataskydd	**Skydd av privatlivet** är en grundläggande rättighet för alla. För att skydda personers privatliv är också behandlingen av uppgifter om dem, det vill säga **personuppgifter**, strikt reglerad. Detta brukar kallas dataskydd.
GDPR	GDPR dvs. General Data Protection Regulation (EU:s allmänna dataskyddsförordning) är en dataskyddsförordning som **reglerar behandlingen av personuppgifter** och har tillämpats i alla EU-länder sedan våren 2018.
Informations-säkerhet	Med informationssäkerhet avses administrativa och tekniska åtgärder genom vilka det säkerställs informationens a) **konfidentialitet**, dvs. att information är tillgänglig endast för dem som har rätt att använda den b) **integritet**, dvs. att informationen inte kan ändras av andra än dem som har rätt till detta samt c) **användbarhet**, dvs. att informationen och informationssystemen kan utnyttjas av dem som har rätt att använda informationen och systemen.

Kategorisering av data

DATASKYDD
CENTRALA BEGREPP

Personuppgifter

All information utifrån vilken man **direkt eller indirekt kan identifiera en person**. Personuppgifter är exempelvis **namn**, **personbeteckning** och **kontaktuppgifter**, men också **bilder** eller **videoinspelningar** kan vara personuppgifter, om en person kan identifieras i dem. Även pseudonymiserade uppgifter är personuppgifter.

Särskilda kategorier av personuppgifter

Sådana uppgifter redogör för personens **ras** eller **etniska ursprung**, **politiska åsikter**, **religiösa** eller **filosofiska övertygelse**, **medlemskap i fackförbund**, **hälsorelaterade uppgifter**, **sexuella läggning** eller **beteende**, eller **genetiska** och **biometriska uppgifter** för identifiering av personen.

Offentlig uppgift

Uppgift som gäller eller **inte gäller en person**, som inte separat definierats som sekretessbelagd enligt lag.

Sekretess-belagd uppgift

Uppgift som gäller eller inte gäller en person, som **separat definierats som sekretessbelagd enligt lag**. Exempelvis uppgifter om **hälsa**.

Pseudonymi-serade uppgifter

Pseudonymisering betyder att **personuppgifter inte längre kan kopplas till en viss person** utan att använda tilläggsinformation, som förvaras separat från personuppgifterna. Pseudonymisering används i allmänhet vid **forskning** och **statistikföring**. Det handlar också om pseudonymisering exempelvis om en **lärare registrerar elever eller studerande i en elektronisk lärmiljö med signaturer** eller andra användarnamn, men fortfarande kan skilja mellan eleverna med hjälp av en lista över deras namn och användarnamn.

Anonyma uppgifter

Med anonyma uppgifter avses **uppgifter som inte är kopplade till en fysisk person som har identifierats eller kan identifieras**. Med anonymisering avses olika åtgärder som vidtas med personuppgifter, som leder till att möjligheten att identifiera en person förhindras oåterkalleligt. För att anonymisera uppgifter kan man exempelvis förenkla informationsmaterialet eller ta bort bakgrundsvariabler så att personen inte längre kan identifieras. Anonymiserat material är exempelvis statistisk information om fostran och undervisning, där enskilda barn, elever eller vårdnadshavare inte går att identifiera.

DATASKYDD
CENTRALA BEGREPP

Personer och aktörer

Dataskydds-ombud

Person, vars utnämning, position och uppgifter regleras separat i dataskyddsförordningen. Ett dataskyddsombud **följer** bl.a. **behandlingen av personuppgifter** och **hjälper till att beakta dataskyddslagstiftningen i registeransvarigens verksamhet**.

Personuppgifts-ansvarig

En personuppgiftsansvarig är en aktör som **ansvarar för behandling av personuppgifter som den själv utför eller som utförs för dess räkning**. Den personuppgiftsansvariga är en person eller organisation som **definierar syftena och metoderna för behandling av personuppgifter**, det vill säga **varför och hur personuppgifter behandlas**. En anordnare av fostran och utbildning är personuppgiftsansvarig då den använder uppgifter om barn, elever och vårdnadshavare för att ordna undervisningen och fostran.

Personuppgifts-biträde

En person eller organisation som behandlar personuppgifter för en personuppgiftsansvarigs räkning. **Ett personuppgiftsbiträde är** ofta exempelvis **en leverantör av IT-tjänster**, som en anordnare har köpt ett elevadministrationssystem med relaterade stödtjänster av. Den personuppgiftsansvariga och personuppgiftsbiträdet ska ha ett avtal om behandling av personuppgifter.

Registrerad

Den person, till exempel ett barn, en elev eller en vårdnadshavare, **som personuppgifter gäller**.

Gemensam personuppgifts-ansvarig

När **flera personuppgiftsansvariga definierar syftena och metoderna för behandlingen gemensamt** kallas det för gemensamt personuppgiftsansvar. Regler för gemensamt personuppgiftsansvar och ansvarsfördelning mellan exempelvis Utbildningsstyrelsen och utbildningsanordnare i samband med det finns exempelvis i fråga om informationsresursen inom småbarnspedagogik (VARDA) och den nationella informationsresursen för undervisning och utbildning (KOSKI).

DATASKYDD

CENTRALA BEGREPP

Skyldigheter

Dataskydds-principer

Dataskyddsprinciperna ska alltid följas vid behandling av personuppgifter. Dataskyddsprinciperna **definieras i dataskyddsförordningen**. Principerna är **laglighet**, **korrekthet** och **transparens**, **ändamålsbegränsning**, **uppgiftsminimering**, **korrekthet**, **integritet** och **konfidentialitet** samt **lagrings-minimering**.

Grund för behandling

Laglighetsprincipen förutsätter att **den personuppgiftsansvariga har en lagenlig grund för behandlingen av uppgifterna**. Grunderna **regleras i dataskyddsförordningen**, och man hänvisar ofta till dem som grund för behandlingen eller behandlingens rättsliga grund. Grunder är exempelvis en lagstadgad skyldighet och samtycke.

Personuppgifts-incident

En **händelse** som leder till att **personuppgifter förstörs**, **försvinner**, **ändras**, **olovligen överlåts** eller **hamnar i händerna på en aktör som saknar rätt att behandla dem**. Det kan till exempel vara frågan om en överbelastningsattack, ett skadeprogram, ett dataintrång eller -läckage, att inloggningsuppgifter hamnar i fel händer eller stöld av arbetsredskap såsom en dator eller en telefon. En personuppgifts-incident ska meddelas till dataombudsmannens byrå och/eller till den registrerade i enlighet med lagen.

Konsekvens-bedömning

När vissa kriterier uppfylls ska den personuppgiftsansvariga göra en **konsekvensbedömning med avseende på dataskydd** innan behandlingen inleds. En konsekvensbedömning kan komma i fråga exempelvis när man vill ta i bruk nya digitala miljöer.

Personregister

Med ett register avses vilken **samling av information** som helst **som innehåller strukturerade personuppgifter**, och ur vilken man kan få information på vissa grunder. Exempelvis ett kundregister för småbarnspedagogiken, ett elevregister för den grundläggande utbildningen eller ett elevhälsoregister.

Den registrerades uppgifter

Den registrerades rättigheter regleras i dataskyddsförordningen och dataskyddslagen. **Den registrerades rättigheter är situationsbundna** och beror ofta på vilken grunden för behandlingen av uppgifterna är. Den registrerade kan exempelvis ha rätt att kräva att felaktiga eller onödiga uppgifter om hen tas bort ur ett personregister. En registrerad persons begäran om att utöva sina rättigheter ska besvaras inom en viss tid.

Berätta om behandlingen för den registrerade

Den personuppgiftsansvariga ska **informera de registrerade om behandlingen av deras personuppgifter** i enlighet med vad som sägs i dataskyddsförordningen och dataskyddslagen. Anordnare av fostran och utbildning tillhandahåller i allmänhet informationen genom särskilda **dataskydds-** eller motsvarande **beskrivningar**.

Inbyggt dataskydd och dataskydd som standard

Den personuppgiftsansvariga ska innan behandlingen av personuppgifter inleds säker**ställa att kraven gällande dataskydd** har beaktats i behandlingen och att den **planerade behandlingen är laglig**.

OPETUSHALLITUS
UTBILDNINGSSTYRELSEN

The Artificial Intelligence Act

Oacceptabelt: Applikationer som omfattar subliminala tekniker, exploaterande system eller sociala poängsystem som används av offentliga myndigheter är strikt förbjudna. Förbjudet är också alla realtidsbiometriska identifieringssystem som används av brottsbekämpande myndigheter på offentligt tillgängliga platser.

AI-system för social för att rangordna medborgare efter beteende.

Högrisk: Dessa inkluderar applikationer relaterade till transport, utbildning, sysselsättning och välfärd, bland annat. Innan ett högrisk AI-system får sättas på marknaden eller tas i bruk inom EU måste företag genomföra en "överensstämmelse-bedömning" och uppfylla en lång lista av krav för att säkerställa att systemet är säkert. Som en pragmatisk åtgärd kräver förordningen även att Europeiska kommissionen skapar och upprätthåller en offentligt tillgänglig databas där leverantörer är skyldiga att tillhandahålla information om sina högrisk-AI-system för att säkerställa transparens för alla intressenter.

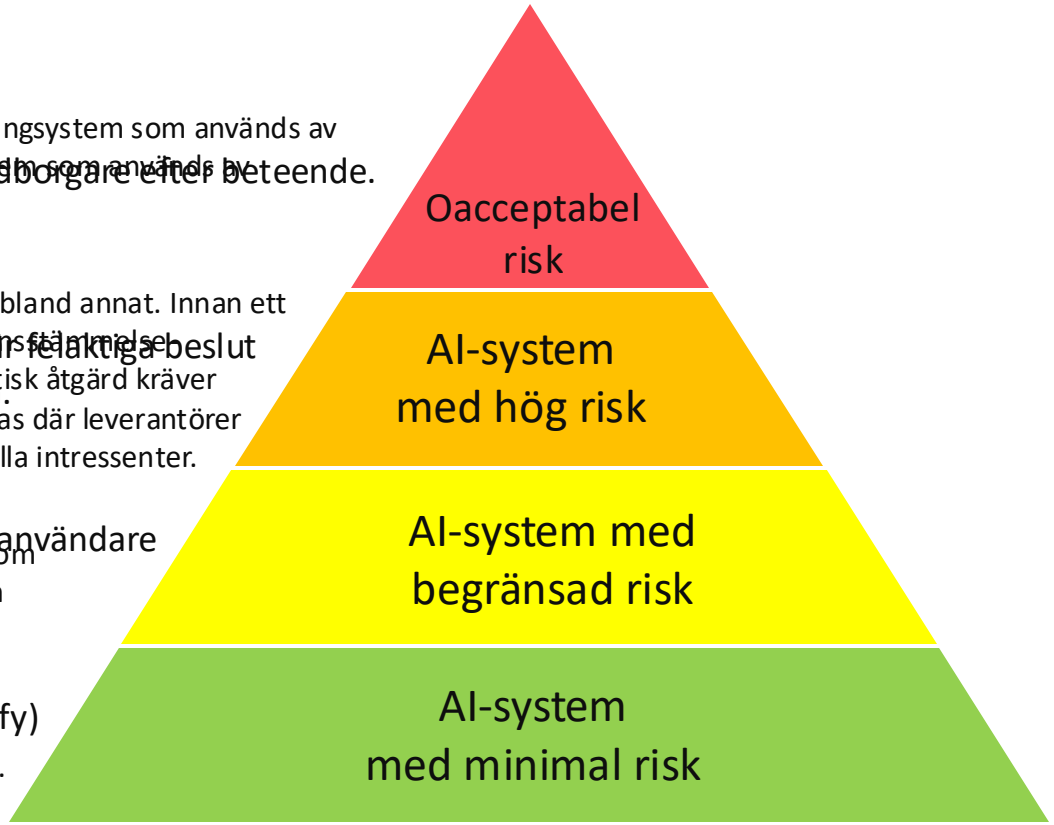
AI för medicinsk diagnostik och behandling, där felaktiga beslut kan ha stora konsekvenser för patienters hälsa.

Begränsad risk: Dessa AI-system måste uppfylla specifika transparenskrav. Till exempel ska en individ som interagerar med en chatbot informeras om att de kommunicerar med en maskin, så att de kan välja om de vill fortsätta eller begära att prata med en människa istället.

AI-baserade chatbotar som kommunicerar med kunder på en webbplats, där användare måste informeras om att de interagerar med en AI och inte en människa.

Minimal risk: Dessa applikationer är redan allmänt utbredda och utgör majoriteten av de AI-system vi interagerar med idag. Exempel på dessa är spamfilter, AI-drivna datorspel och system för lagerhantering.

AI som genererar spellistor på musikstreamingplattformar (t.ex. Spotify) baserat på användarens tidigare lyssnande.



https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=OJ:L_202401689

I **utbildningskontexten** är **system med hög risk** till exempel system som är avsedda att användas:

- för att utvärdera läranderesultat, även när dessa resultat används för att styra personers lärandeprocess inom småbarnspedagogiken och utbildning
- för att bedöma den utbildningsnivå som en person kommer att erhålla eller kommer att kunna få tillgång till inom småbarnspedagogiken eller utbildningen
- för att övervaka och upptäcka förbjudet beteende under provtillfällen inom småbarnspedagogiken och utbildningen

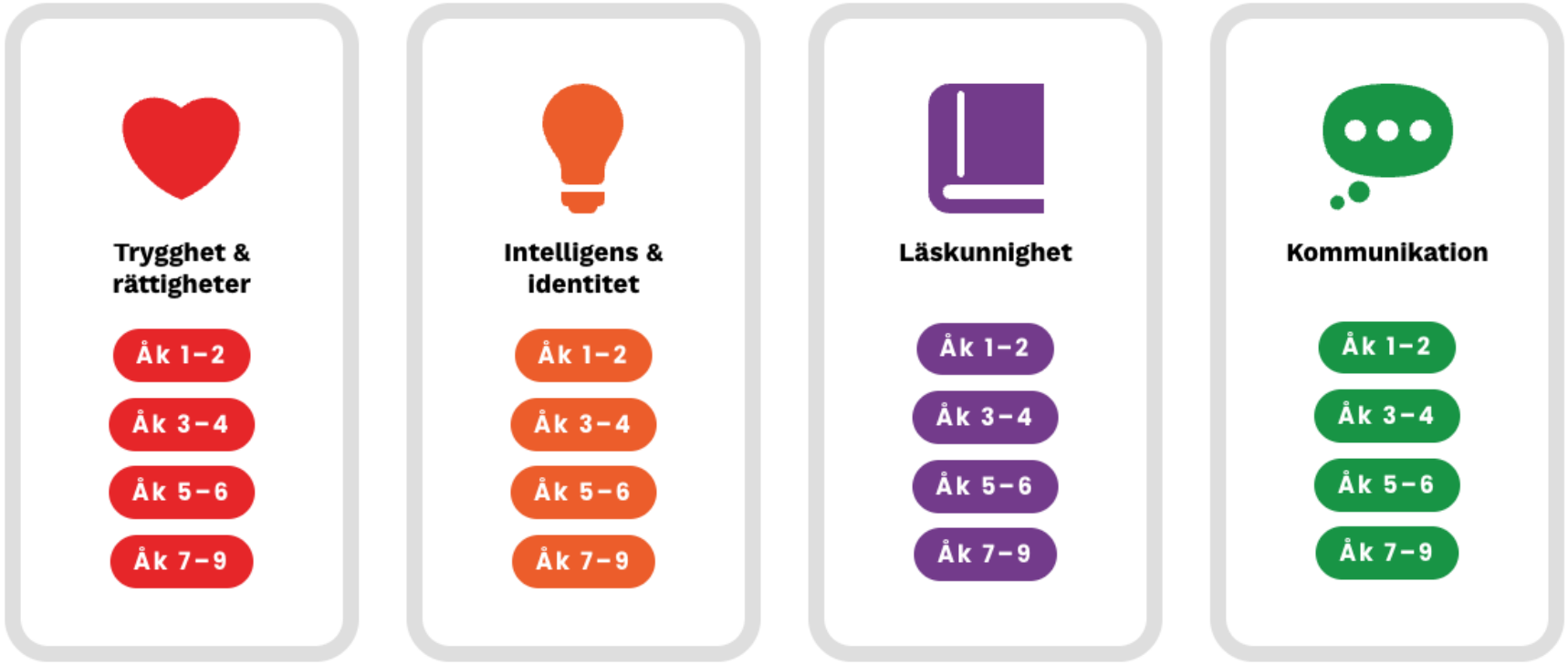
Ett AI-system avses dock **inte som ett system med hög risk** och det anses **inte ha någon väsentlig påverkan på resultatet av beslutsfattande**, om något av följande villkor uppfylls:

- Systemet förbättrar resultatet av tidigare utförd mänsklig verksamhet, till exempel förbättrar det språk som används i tidigare utarbetade dokument.
- Systemet är avsett att upptäcka beslutsmönster eller avvikelser från tidigare beslutsmönster, till exempel kan lärares betygsättningsmönster användas för att i efterhand kontrollera om läraren har avvikit från betygsättningsmönstret. Syftet med systemet ska dock inte vara att ersätta eller påverka en tidigare slutförd mänsklig bedömning utan ordentlig mänsklig granskning.
- Systemet ska endast utföra förberedande uppgifter, så att den eventuella effekten av systemets utdata är mycket liten med tanke på uppgiften. Bland annat besluten fattas i detta fall av människan."

AI-system
med hög risk

Teman på #somesmart

VASA ÖVNINGSSKOLA



somesmart.abo.fi

DIMENSION 1• **KOMPETENSOMRÅDE**

4. SÄKERHET

DIMENSION 2 • **KOMPETENS**

1. SKYDDA UTRUSTNING

Att skydda utrustning och digitalt innehåll och att förstå risker och hot i digitala miljöer.

Att känna till trygghets- och säkerhetsåtgärder och att ta tillbörlig hänsyn till tillförlitlighet och integritet.

GRUNDLÄGGANDE	1	På grundläggande nivå och med vägledning, kan jag:	• identifiera enkla sätt att skydda min utrustning och mitt digitala innehåll och • särskilja enkla risker och hot i digitala miljöer. • välja enkla trygghets- och säkerhetsåtgärder samt • identifiera enkla sätt att ta tillbörlig hänsyn till tillförlitlighet och integritet.
	2	På grundläggande nivå och självständigt och med lämplig vägledning där det behövs, kan jag:	• identifiera enkla sätt att skydda min utrustning och mitt digitala innehåll och • särskilja enkla risker och hot i digitala miljöer. • välja enkla trygghets- och säkerhetsåtgärder samt • identifiera enkla sätt att ta tillbörlig hänsyn till tillförlitlighet och integritet.
MELLANLIGGANDE	3	På egen hand och för att lösa okomplicerade problem, kan jag:	• visa på väl definierade och rutinmässiga sätt att skydda min utrustning och mitt digitala innehåll samt • särskilja väl definierade och rutinmässiga risker och hot i digitala miljöer samt • välja väl definierade och rutinmässiga trygghets- och säkerhetsåtgärder. • visa på väl definierade och rutinmässiga sätt att ta tillbörlig hänsyn till tillförlitlighet och integritet.
	4	Självständigt, utifrån mina egna behov och för att lösa väl definierade och icke-rutinmässiga problem, kan jag:	• organisera sätt att skydda min utrustning och mitt digitala innehåll samt • särskilja risker och hot i digitala miljöer samt • välja trygghets- och säkerhetsåtgärder. • förklara hur man kan ta tillbörlig hänsyn till tillförlitlighet och integritet.

DIMENSION 1 • **KOMPETENSOMRÅDE**

4. SÄKERHET

DIMENSION 2 • **KOMPETENS**

1. SKYDDA UTRUSTNING

Att skydda utrustning och digitalt innehåll och att förstå risker och hot i digitala miljöer.

Att känna till trygghets- och säkerhetsåtgärder och att ta tillbörlig hänsyn till tillförlitlighet och integritet.

AVANCERAD	5	Såväl som att vägleda andra, kan jag:	• tillämpa olika sätt att skydda utrustning och digitalt innehåll samt • särskilja en variation av risker och hot i digitala miljöer. • tillämpa trygghets- och säkerhetsåtgärder. • använda sig av olika sätt att ta tillbörlig hänsyn till tillförlitlighet och integritet.
	6	På avancerad nivå, utifrån mina egna och utifrån andras behov och i komplexa sammanhang, kan jag:	• välja det lämpligaste skyddet för utrustning och digitalt innehåll samt • särskilja risker och hot i digitala miljöer. • välja de lämpligaste trygghets- och säkerhetsåtgärderna. • bedöma de lämpligaste sätten att ta tillbörlig hänsyn till tillförlitlighet och integritet.
HÖGT SPECIALISERAD	7	På högt specialiserad nivå, kan jag:	• skapa lösningar på komplexa problem med begränsad definition, relaterade till att skydda utrustning och digitalt innehåll, att hantera risker och hot, att tillämpa trygghets- och säkerhetsåtgärder samt att ta tillbörlig hänsyn tillförlitlighet och integritet i digitala miljöer. • integrera mina kunskaper för att bidra till professionell praxis och kunskap samt vägleda andra i att skydda sin utrustning.
	8	På den mest avancerade och specialiserade nivån, kan jag:	• skapa lösningar för att klara komplexa problem med flera interagerande faktorer, relaterade till att skydda utrustning och digitalt innehåll, att hantera risker och hot, att tillämpa trygghets- och säkerhetsåtgärder samt att ta tillbörlig hänsyn tillförlitlighet och integritet i digitala miljöer. • föreslå nya idéer och processer till fältet.

DIMENSION 4 • EXEMPEL PÅ KUNSKAP, FÄRDIGHETER OCH ATTITYD

NYTT I 2.2

KUNSKAP

166. Vet att ett sätt att undvika de negativa konsekvenserna av att någon kommer över ens konto (t.ex. blir hackat) är att använda olika starka lösenord för olika onlinetjänster.
167. Känner till åtgärder för att skydda enheter (t.ex. lösenord, fingeravtryck, kryptering) och att hindra andra (t.ex. en tjuv, kommersiell organisation, myndighet) från att få tillgång till alla data.
168. Är medveten om vikten av att hålla operativsystemet och applikationer (t.ex. webbläsaren) uppdaterade för att åtgärda säkerhetsluckor och skydda mot skadlig mjukvara (dvs. malware).
169. Vet att brandväggar blockerar vissa typer av nätverkstrafik, med syftet att förhindra olika säkerhetsrisker (t.ex. fjärrinloggning).
170. Är medveten om olika typer av risker i digitala miljöer, såsom identitetsstöld (t.ex. någon som utför bedrägerier eller andra brott med hjälp av en annan persons personuppgifter), bedrägerier (t.ex. ekonomiska bedrägerier där offren luras till att skicka pengar), attacker med skadlig programvara (t.ex. ransomware).

FÄRDIGHETER

171. Vet hur man antar en lämplig strategi för cyberhygien vad gäller lösenord (t.ex. att välja starka lösenord som är svåra att gissa) och att hantera dem säkert (t.ex. med hjälp av en lösenordshanterare).
172. Vet hur man installerar och aktiverar skyddsprogram och -tjänster (t.ex. antivirus, antimalware, brandvägg) för att förvara digitalt innehåll och personuppgifter säkrare.
173. Vet hur man aktiverar tvåfaktorsautentisering när den är tillgänglig (t.ex. med hjälp av engångslösenord eller koder tillsammans med åtkomstuppgifter).
174. . Vet hur man kan kontrollera vilka personuppgifter en app har tillgång till på mobiltelefonen och baserat på det avgöra om man vill installera den och i så fall göra lämpliga inställningar.
175. Kan kryptera känsliga data som lagras på en personlig enhet eller i en molnlagringstjänst.
176. Kan ta till lämpliga åtgärder som svar på ett säkerhetsintrång (dvs. ett tillbud som leder till obehörig åtkomst av digitala data, applikationer, nätverk eller enheter, eller att personuppgifter såsom inloggningsuppgifter eller lösenord läcker).

ATTITYD

177. Vaksam på att inte lämna datorer eller mobila enheter utan tillsyn på offentliga platser (t.ex. delade arbetsplatser, restauranger, tåg, bil).
178. Väger fördelarna med att använda biometrisk identifiering (t.ex. fingeravtryck, ansiktsigenkänning) mot riskerna, eftersom dessa tekniker kan ha oavsiktlig påverkan på säkerheten. Om biometrisk information läcker eller hackas blir den äventyrad och kan leda till identitetsbedrägeri.
179. Angelägen om att skydda sig själv, såsom att inte göra ekonomiska transaktioner eller sköta bankärenden över öppna, trådlösa nätverk.

DIMENSION 5 • ANVÄNDNINGSFALL

AVANCERAD NIVÅ 5

PÅ ARBETSPLATSEN: använda ett Twitter-konto för att dela information om min organisation

- Jag kan skydda organisationens Twitter-konto med olika metoder (t.ex. ett starkt lösenord, kontrollera de senaste inloggningarna) och visa nya kollegor hur man gör det.
- Jag kan upptäcka riskerna såsom att få tweets och meddelanden från följare med falska profiler eller försök till nätfiske (phishing).
- Jag kan ta till åtgärder för att undvika riskerna (t.ex. kontrollera sekretessinställningarna).
- Jag kan också hjälpa mina kollegor att upptäcka risker och hot då de använder Twitter..

I UTBILDNING: använda skolans digitala plattform för att dela information om intressanta ämnen.

- Jag kan skydda information, data och innehåll på skolans digitala plattform (t.ex. ett starkt lösenord, kontrollera de senaste inloggningarna).
- Jag kan upptäcka olika risker och hot då jag använder skolans digitala plattform och kan ta till åtgärder för att undvika dem (t.ex. hur man kan granska en bilaga för virus innan man laddar ner den).
- Jag kan också hjälpa mina klasskompisar upptäcka risker och hot då de använder den digitala plattformen på sina enheter (t.ex. kontrollera vem som kan komma åt filerna).

DIMENSION 1• **KOMPETENSOMRÅDE**

4. SÄKERHET

DIMENSION 2 • **KOMPETENS**

4.2 SKYDDA PERSONUPPGIFTER OCH INTEGRITET

Att skydda personuppgifter och integritet i digitala miljöer.

Att förstå hur man använder och delar personligt identifierbar information samtidigt som man skyddar sig själv och andra från att ta skada.

Att förstå att digitala tjänster använder en ”integritetspolicy” för att informera om hur personuppgifter används.

GRUNDLÄGGANDE	1	På grundläggande nivå och med vägledning, kan jag:	• välja enkla sätt att skydda mina personuppgifter och min integritet i digitala miljöer, • identifiera enkla sätt att använda och dela personligt identifierbar information samtidigt som jag skyddar mig själv och andra från att ta skada. • identifiera enkla integritetsskyddsregler för hur personuppgifter används i digitala tjänster.
	2	På grundläggande nivå och självständigt och med lämplig vägledning där det behövs, kan jag:	• välja enkla sätt att skydda mina personuppgifter och min integritet i digitala miljöer, • identifiera enkla sätt att använda och dela personligt identifierbar information samtidigt som jag skyddar mig själv och andra från att ta skada. • identifiera enkla integritetsskyddsregler för hur personuppgifter används i digitala tjänster..
MELLANLIGGANDE	3	På egen hand och för att lösa okomplicerade problem, kan jag:	• förklara väl definierade och rutinmässiga sätt att skydda mina personuppgifter och min integritet i digitala miljöer och • förklara väl definierade och rutinmässiga sätt att använda och dela personligt identifierbar information samtidigt som jag skyddar mig själv och andra från att ta skada. • visa upp väl definierade och rutinmässiga integritetsskyddsregler för hur personliga data används i digitala tjänster.
	4	Självständigt, utifrån mina egna behov och för att lösa väl definierade och icke-rutinmässiga problem, kan jag:	• diskutera sätt att skydda mina personuppgifter och min integritet i digitala miljöer och • diskutera sätt att använda och dela personligt identifierbar information samtidigt som jag skyddar mig själv och andra från att ta skada. • visa upp integritetsskyddsregler för hur personliga data används i digitala tjänster.

DIMENSION 1• **KOMPETENSOMRÅDE**

4. SÄKERHET

DIMENSION 2 • **KOMPETENS**

4.2 SKYDDA PERSONUPPGIFTER OCH INTEGRITET

Att skydda personuppgifter och integritet i digitala miljöer.

Att förstå hur man använder och delar personligt identifierbar information samtidigt som man skyddar sig själv och andra från att ta skada.

Att förstå att digitala tjänster använder en ”integritetspolicy” för att informera om hur personuppgifter används.

AVANCERAD	5	Såväl som att vägleda andra, kan jag:	• tillämpa olika sätt att skydda mina personuppgifter och min integritet i digitala miljöer, • tillämpa olika specifika sätt att dela mina uppgifter samtidigt som jag skyddar mig själv och andra från att ta skada. • förklara integritetsskyddsregler för hur personuppgifter används i digitala tjänster..
	6	På avancerad nivå, utifrån mina egna och utifrån andras behov och i komplexa sammanhang, kan jag:	• välja de lämpligaste sätten sätt att skydda mina personuppgifter och min integritet i digitala miljöer samt • utvärdera de lämpligaste sätten att använda och dela personligt identifierbar information samtidigt som jag skyddar mig själv och andra från att ta skada. • utvärdera lämpligheten hos de integritetsskyddsregler som berör användningen av personuppgifter.
HÖGT SPECIALISERAD	7	På högt specialiserad nivå, kan jag:	• skapa lösningar på komplexa problem med begränsad definition, relaterade till att skydda mina personuppgifter och min integritet i digitala miljöer, till att använda och dela mina uppgifter samtidigt som jag skyddar mig själv och andra från att ta skada och till integritetsskyddsregler som berör användningen av personuppgifter. • integrera mina kunskaper för att bidra till professionell praxis och kunskap samt vägleda andra i att skydda sina personuppgifter och sin integritet.
	8	På den mest avancerade och specialiserade nivån, kan jag:	• skapa lösningar för att klara komplexa problem med flera interagerande faktorer, relaterade till att skydda mina personuppgifter och min integritet i digitala miljöer, till att använda och dela mina uppgifter samtidigt som jag skyddar mig själv och andra från att ta skada och till integritetsskyddsregler som berör användningen av personuppgifter. • föreslå nya idéer och processer till fältet.

DIMENSION 4 • **EXEMPEL PÅ KUNSKAP, FÄRDIGHETER OCH ATTITYD**

NYTT I 2.2

KUNSKAP

180. Känner till att säker elektronisk identifiering är en nyckelegenskap skapad för att möjliggöra säkrare delning av personuppgifter med tredje part i samband med privata transaktioner och transaktioner inom den offentlig sektorn.
181. Vet att integritetspolicyn för en app eller tjänst bör förklara vilka personuppgifter den samlar in (t.ex. namn, enhetens märke, användarens geografiska position) och om data delas med tredje part.
182. Vet att hanteringen av personuppgifter är föremål för lokala föreskrifter, såsom EU:s dataskyddsförordning (GDPR (t.ex. utgör röstkommunikation med en virtuell assistent personuppgifter enligt GDPR och kan utsätta användare för vissa dataskydds-, integritets- och säkerhetsrisker). (AI)

FÄRDIGHETER

183. Vet hur man kan identifiera misstänkta epostmeddelanden som försöker komma över känslig information (t.ex. personuppgifter, bankidentifikation) eller som kan innehålla skadlig programvara. Vet att denna typ av mejl ofta utformas för att lura personer som inte gör en noggrann granskning och som därför är mer mottagliga för bedrägerier genom att innehålla avsiktliga fel som hindrar vaksamma personer från att klicka på dem.
184. Vet hur man tillämpar grundläggande säkerhetsåtgärder i samband med nätbetalningar (t.ex. att aldrig skicka en inskannad bild av kreditkort eller ge ut ett korts pinkod).
185. Vet hur man använder elektronisk identifiering för tjänster som handhas av myndigheter eller offentliga sektorn (t.ex. att fylla i skattedeklarationen, söka socialstöd, ansöka om intyg) och den privata sektorn, såsom bank- och transporttjänster.
186. Vet hur man använder digitala certifikat som utges av certifierande myndigheter (t.ex. digitala certifikat för autentisering och digitala underskrifter som lagras på nationella id-kort).

ATTITYD

187. Väger fördelarna mot riskerna innan man låter tredje parter hantera personuppgifter (t.ex. inser att en röstassistent på en telefon som används för att ge instruktioner till en robotdammsugare kan ge tredje part – företag, myndigheter, nätbrottslingar – tillgång till data). (AI)
188. Känner sig säker då man utför nättransaktioner efter att ha vidtagit lämpliga trygghets- och säkerhetsåtgärder.

DIMENSION 5 • **ANVÄNDNINGSFALL**

AVANCERAD NIVÅ 6

PÅ ARBETSPLATSEN: : använda ett Twitter-konto för att dela information om min organisation

- Jag kan välja det lämpligaste sättet att skydda mina kollegors personuppgifter (t.ex. adress, telefonnummer) när jag delar digitalt innehåll (t.ex. en bild) på företagets Twitter-konto.
- Jag kan skilja mellan lämpligt och olämpligt digitalt innehåll att dela på företagets Twitter-konto så att min och mina kollegors integritet inte kränks.
- Jag kan avgöra om personuppgifter på företagets Twitter-konto används i enlighet med dataskyddsförordningen GDPR och dess princip om ”rätten att bli bortglömd”.
- Jag kan hantera komplexa situationer som kan uppstå i relation till personuppgifter i min organisation på Twitter genom att t.ex. ta bort bilder eller namn för att skydda personlig information, i enlighet med dataskyddsförordningen GDPR och dess princip om ”rätten att bli bortglömd”.

I UTBILDNING: använda skolans digitala plattform för att dela information om intressanta ämnen

- Jag kan välja det lämpligaste sättet att skydda mina personuppgifter (t.ex. adress, telefonnummer) innan jag delar information på skolans digitala plattform.
- Jag kan skilja mellan lämpligt och olämpligt digitalt innehåll att dela på skolans digitala plattform så att min och mina klasskompisars integritet inte kränks.
- Jag kan avgöra om det sätt på vilket mina personuppgifter används på skolans plattform är lämpligt och acceptabelt i relation till mina rättigheter och min integritet.
- Jag kan övervinna komplexa situationer som kan uppstå gällande mina och mina klasskompisars personuppgifter när vi använder skolans digitala plattform, såsom att personuppgifter inte används i enlighet med plattformens integritetspolicy.

DIMENSION 1 • **KOMPETENSOMRÅDE**

4. SÄKERHET

DIMENSION 2 • **KOMPETENS**

4.3 SKYDDA HÄLSA OCH VÄLBEFINNANDE

Att kunna undvika hälsorisker och hot mot det fysiska och psykiska välbefinnandet när man använder digitala tekniker.
Att kunna skydda sig själv och andra från möjliga faror i digitala miljöer (t.ex. nätmobbning).
Att känna till digitala tekniker för socialt välbefinnande och social inkludering.

GRUNDLÄGGANDE	1	På grundläggande nivå och med vägledning, kan jag:	• särskilja enkla sätt att undvika hälsorisker och hot mot fysiskt och psykiskt välbefinnande vid användning av digitala tekniker. • välja enkla sätt att skydda mig själv från möjliga faror i digitala miljöer. • identifiera enkla digitala tekniker för socialt välbefinnande och social inkludering.
	2	På grundläggande nivå och självständigt och med lämplig vägledning där det behövs, kan jag:	• särskilja enkla sätt att undvika hälsorisker och hot mot fysiskt och psykiskt välbefinnande vid användning av digitala tekniker. • välja enkla sätt att skydda mig själv från möjliga faror i digitala miljöer. • identifiera enkla digitala tekniker för socialt välbefinnande och social inkludering.
MELLANLIGGANDE	3	På egen hand och för att lösa okomplicerade problem, kan jag:	• förklara väl definierade och rutinmässiga sätt att undvika hälsorisker och hot mot fysiskt och psykiskt välbefinnande vid användning av digitala tekniker. • välja väl definierade och rutinmässiga sätt att skydda mig själv från möjliga faror i digitala miljöer. • identifiera väl definierade och rutinmässiga digitala tekniker för socialt välbefinnande och social inkludering.
	4	Självständigt, utifrån mina egna behov och för att lösa väl definierade och icke-rutinmässiga problem, kan jag:	• förklara sätt att undvika hot mot fysisk och psykisk hälsa relaterat till användning av digitala tekniker. • välja sätt att skydda mig själv och andra från faror i digitala miljöer. • diskutera om digitala tekniker relaterat till socialt välbefinnande och social inkludering.

DIMENSION 1• **KOMPETENSOMRÅDE**

4. SÄKERHET

DIMENSION 2 • **KOMPETENS**

4.3 SKYDDA HÄLSA OCH VÄLBEFINNANDE

Att kunna undvika hälsorisker och hot mot det fysiska och psykiska välbefinnandet när man använder digitala tekniker.
Att kunna skydda sig själv och andra från möjliga faror i digitala miljöer (t.ex. nätmobbning).
Att känna till digitala tekniker för socialt välbefinnande och social inkludering.

AVANCERAD	5	Såväl som att vägleda andra, kan jag:	• visa olika sätt att undvika hälsorisker och hot mot det fysiska och psykiska välbefinnandet vid användning av digitala tekniker. • tillämpa olika sätt att skydda mig själv och andra från faror i digitala miljöer. • visa olika digitala tekniker för socialt välbefinnande och social inkludering.
	6	På avancerad nivå, utifrån mina egna och utifrån andras behov och i komplexa sammanhang, kan jag:	• särskilja de lämpligaste sätten att undvika hälsorisker och hot mot det fysiska och psykiska välbefinnandet vid användning av digitala tekniker. • anpassa de lämpligaste sätten att skydda mig själv och andra från faror i digitala miljöer. • variera användningen av digitala tekniker för socialt välbefinnande och social inkludering.
HÖGT SPECIALISERAD	7	På högt specialiserad nivå, kan jag:	• skapa lösningar på komplexa problem med begränsad definition, relaterade till att undvika hälsorisker och hot mot det fysiska och psykiska välbefinnandet vid användning av digitala tekniker, till att skydda mig själv och andra från faror i digitala miljöer och till användningen av digitala tekniker för socialt välbefinnande och social inkludering. • integrera mina kunskaper för att bidra till professionell praxis och kunskap samt vägleda andra i att skydda sin hälsa.
	8	På den mest avancerade och specialiserade nivån, kan jag:	• skapa lösningar för att klara komplexa problem med flera interagerande faktorer, relaterade till att undvika hälsorisker och hot mot det fysiska och psykiska välbefinnandet vid användning av digitala tekniker, till att skydda mig själv och andra från faror i digitala miljöer och till användningen av digitala tekniker för socialt välbefinnande och social inkludering. • föreslå nya idéer och processer till fältet.

DIMENSION 4 • **EXEMPEL PÅ KUNSKAP, FÄRDIGHETER OCH ATTITYD**

NYTT I 2.2

KUNSKAP

189. Är medveten om vikten av att balansera användningen av digitala tekniker med icke-användning som en möjlighet, eftersom många faktorer i det digitala livet kan inverka på hälsan, välbefinnandet och livskvalité.
190. Känner till tecken på digitala beroenden (t.ex. att tappa kontrollen, abstinensbesvär, humörsvängningar) och att digitala beroenden kan orsaka psykiskt och fysiskt lidande.
191. Är medveten om att det för många digitala hälsoapplikationer inte finns några officiella licenskrav likt inom reguljär medicin.
192. Är medveten om att en del applikationer på digitala enheter (t.ex. telefonen) kan främja hälsosamma vanor genom att bevaka/följa upp/styra och uppmärksamma användaren på hälsotillstånd (t.ex. fysiska, känslomässiga, psykologiska). Vissa aktiviteter eller bildspråk som föreslås av sådana applikationer kan dock också ha negativa effekter på den fysiska eller mentala hälsan (t.ex. kan "idealiserade" kroppsbilder orsaka ångest).
193. Förstår att nätmobbning är mobbning med hjälp av digitala teknologier (dvs. ett upprepat beteende som syftar till att skrämma, uppröra eller skämma ut dem som beteendet riktas mot).
194. Vet att den s.k. avhämningseffekten online ("online disinhibition effect") innebär att man inte är lika återhållsam när man kommunicerar online som när man kommunicerar ansikte mot ansikte. Detta kan leda till en ökad tendens för olämpligt och ohämmat beteende, exempelvis i form av så kallad "flaming" (t.ex. att använda kränkande språk, publicera förolämpningar på nätet).
195. Är medveten om att utsatta grupper (t.ex. barn, de med bristande sociala färdigheter och de med brist på sociala skyddsnätverk) löper en högre risk att falla offer i digitala miljöer (t.ex. nätmobbning, gromning).
196. Är medveten om att digitala verktyg kan skapa nya möjligheter att delta i samhället för utsatta grupper (t.ex. äldre personer, personer med särskilda behov). Digitala verktyg kan också leda till isolering eller uteslutning av dem som inte använder dem.

FÄRDIGHETER

197. Vet hur man både för egen och andras del kan tillämpa en variation av strategier för att styra och begränsa digital användning (t.ex. överenskommelser om skärmfria tider, tillgång till enheter för barn, tidsbegränsningar och filter).
198. Vet hur man upptäcker inbäddade tekniker för användarupplevelser (t.ex. klickfiske, spelifiering, "nudging") som har utformats för att manipulera och/eller försvaga ens förmåga att kontrollera beslut (t.ex. få användaren att lägga mer tid på onlineaktiviteter, uppmuntra till ökad konsumtion).
199. Kan tillämpa och följa skyddsstrategier för att bekämpa kränkningar online (t.ex. blockera användare, inte reagera/svara, skicka vidare eller spara meddelanden som bevis för rättsliga åtgärder, radera negativa meddelanden för att undvika att se dem upprepade gånger).

ATTITYD

200. Benägen att fokusera på fysiskt och mentalt välbefinnande och undvika de negativa effekterna av digitala medier (t.ex. överanvändning, beroende, tvångsmässigt beteende).
201. Tar ansvar för att skydda både den personliga och kollektiva hälsan och säkerheten när man utvärderar effekterna av medicinska och medicinliknande produkter och tjänster online, eftersom internet är fullt av felaktig och potentiellt hälsofarlig information.
202. Är försiktig med rekommendationer (t.ex. om de kommer från en ansedd källa) och deras avsikter (t.ex. hjälper de verkligen användaren eller uppmuntrar de till användning för att användaren ska exponeras för reklam).

DIMENSION 5 • **ANVÄNDNINGSFALL**

HÖGT SPECIALISERAD NIVÅ 7

PÅ ARBETSPLATSEN: : använda ett Twitter-konto för att dela information om min organisation

- Jag kan skapa en digital kampanj om möjliga hälsofaror med att använda Twitter i arbetssyfte (t.ex. mobbning, beroenden, fysiskt välmående) som kan delas och användas av kollegor och andra inom branschen på deras telefoner och läsplattor.

I UTBILDNING: använda skolans digitala plattform för att dela information om intressanta ämnen

- Jag kan skapa en blogg om nätmobbning och social utstötning för min skolas digitala plattform som hjälper mina klasskompisar att upptäcka och stå emot våld i digitala miljöer.

DIMENSION 1 • **KOMPETENSOMRÅDE**

4. SÄKERHET

DIMENSION 2 • **KOMPETENS**

4.4 SKYDDA MILJÖN

Att vara medveten om miljömässig påverkan från digital teknik och dess användning.

GRUNDLÄGGANDE	1	På grundläggande nivå och med vägledning, kan jag:	• känna igen enkel miljöpåverkan från användningen av digitala tekniker.
	2	På grundläggande nivå och självständigt och med lämplig vägledning där det behövs, kan jag:	• känna igen enkel miljöpåverkan från användningen av digitala tekniker.
MELLANLIGGANDE	3	På egen hand och för att lösa okomplicerade problem, kan jag:	• visa på väl definierad och rutinmässig miljöpåverkan från användningen av digitala tekniker.
	4	Självständigt, utifrån mina egna behov och för att lösa väl definierade och icke-rutinmässiga problem, kan jag:	• diskutera sätt för att skydda miljön från påverkan från användningen av digitala tekniker.

DIMENSION 1 • **KOMPETENSOMRÅDE**

4. SÄKERHET

DIMENSION 2 • **KOMPETENS**

4.4 SKYDDA MILJÖN

Att vara medveten om miljömässig påverkan från digital teknik och dess användning.

AVANCERAD	5	Såväl som att vägleda andra, kan jag:	• visa olika sätt för att skydda miljön från påverkan från användningen av digitala tekniker.
	6	På avancerad nivå, utifrån mina egna och utifrån andras behov och i komplexa sammanhang, kan jag:	• välja de lämpligaste lösningarna för att skydda miljön från påverkan från användningen av digitala tekniker.
HÖGT SPECIALISERAD	7	På högt specialiserad nivå, kan jag:	• skapa lösningar på komplexa problem med begränsad definition, relaterade till att skydda miljön från påverkan från användningen av digitala tekniker. • integrera mina kunskaper för att bidra till professionell praxis och kunskap samt vägleda andra i att skydda miljön.
	8	På den mest avancerade och specialiserade nivån, kan jag:	• skapa lösningar för att klara komplexa problem med flera interagerande faktorer, relaterade till att skydda miljön från påverkan från användningen av digitala tekniker. • föreslå nya idéer och processer till fältet.

DIMENSION 4 • EXEMPEL PÅ KUNSKAP, FÄRDIGHETER OCH ATTITYD

NYTT I 2.2

KUNSKAP

203. Är medveten om den miljöpåverkan som vardagliga digitala handlingar har (t.ex. att streama video som förlitar sig på dataöverföring), och att den påverkan består av energiåtgång och koldioxidutsläpp från utrustning, nätverksinfrastruktur och datacenter.
204. Är medveten om den miljöpåverkan som produktionen av digital utrustning och batterier (t.ex. föroreningar och giftiga biprodukter, energikonsumtion) och att sådan utrustning i slutet av sin livslängd måste kasseras på lämpligt sätt för att minimera deras miljöpåverkan och möjliggöra återanvändning av sällsynta och dyra komponenter och naturresurser.
205. Är medveten om att vissa elektronikkomponenter och digital utrustning kan ersättas för att förlänga deras livstid eller prestanda, medan andra kan vara avsiktligt designade att sluta fungera efter en viss tid (planerad inkurans).
206. Känner till "gröna" beteenden att följa vid köp av digital utrustning, t.ex. väljer produkter som har en lägre energikonsumtion under användning och i stand-by-läge, förorsakar mindre föroreningar (produkter som är lättare att plocka isär och återvinna) och är mindre giftiga (begränsad användning av ämnen som är skadliga för miljön och hälsan).
207. Vet att e-handel i och med köp och transport av fysiska varor har en inverkan på miljön (t.ex. koldioxidavtryck från transport, generering av avfall).
208. Är medveten om att digitala tekniker (inklusive AI-baserade sådana) kan bidra till energieffektivitet, t.ex. genom att kontrollera behovet av uppvärmning i hemmet och optimera dess hantering.
209. Är medveten om att vissa aktiviteter (t.ex. att träna AI-lösningar och producera kryptovalutor såsom Bitcoin) är resurskrävande processer när det gäller data och datorkraft. Energiförbrukningen kan därför vara hög, vilket också kan ha en hög miljöpåverkan. (AI)

FÄRDIGHETER

210. Vet hur man tillämpar effektiva lågteknologiska strategier för att skydda miljön, t.ex. att stänga av enheter och wifi, inte skriva ut dokument, reparera och byta ut komponenter för att undvika onödiga utbyten av digitala enheter.
211. Vet hur man kan minska energiförbrukningen för de enheter och tjänster som används, t.ex. genom att ändra kvalitetsinställningarna för videostreamingtjänster, använda wifi i stället för mobildata hemma, stänga appar, optimera e-postbilagor).
212. Vet hur man använder digitala verktyg för att förbättra den miljömässiga och sociala påverkan av ens konsumentbeteende (t.ex. genom att leta efter lokala produkter, gemensamma lösningar och samåkningsalternativ).

ATTITYD

213. Letar fram digital teknik som kan hjälpa till att leva och konsumera på sätt som tar hänsyn till det mänskliga samhällets och den naturliga miljöns hållbarhet.
214. Letar fram information om teknikens miljöpåverkan för att påverka det egna och andras (t.ex. vänners och familjens) beteende till att bli mer ekologiskt ansvariga i användningen av digital teknik.
215. Tänker på en produkts helhetspåverkan på planeten vid val av digitala medel framför fysiska produkter, t.ex. att läsa en bok online kräver inget papper och transportkostnaderna är låga, men å andra sidan innehåller digitala enheter giftiga komponenter och kräver energi för att laddas.
216. Tänker på de etiska konsekvenserna av AI-system över hela deras livscykel, både vad gäller miljöpåverkan (miljökonsekvenser av att producera digital utrustning och tjänster) och samhällspåverkan, t.ex. genom plattformisering av arbete och algoritmisk hantering som kan kränka arbetares integritet eller rättigheter; användning av låglönearbetare för att tagga bilder som ett steg i att träna AI-system. (AI)

DIMENSION 5 • ANVÄNDNINGSFALL

HÖGT SPECIALISERAD NIVÅ 8

PÅ ARBETSPLATSEN: använda ett Twitter-konto för att dela information om min organisation

- Jag kan skapa en illustrerande video som besvarar frågor gällande hållbar användning av digitala enheter i organisationer inom min sektor, för att delas på Twitter och användas av personal och andra inom sektorn.

I UTBILDNING: använda skolans digitala plattform för att dela information om intressanta ämnen

- Jag kan skapa en ny e-bok för att besvara frågor om hållbar användning av digitala enheter i skolan och hemma, och dela den på min skolas digitala plattform för att kunna användas av skolkompisar och deras familjer.

Frågeställningar till gruppdiskussionerna

Framtida utveckling

- Hur skiljer sig användningen av digitala enheter mellan stadierna? Diskutera hur ofta och i vilket sammanhang eleverna använder digitala verktyg och vilka datasäkerhets- och välbefinnandefrågor detta väcker.

- Vilka policyer och riktlinjer har ni för att skydda enheter och persondata i olika stadier? Finns det metoder från andra stadier som ni kan applicera i er egen undervisning?

- Vilka frågeställningar kring hjärnhälsa skulle du vilja lyfta upp i er kommande lärstig?

- Vilka kunskaper och färdigheter skulle ni vilja utveckla vidare för att kunna hantera datasäkerhets- och välbefinnandefrågor ännu bättre i framtiden?