Information till vårdnadshavare på Tryde friskola

…hur vi hanterar och skyddar data/personuppgifter, i enlighet med GDPR.

Information ges ut årligen, samt när nyheter tillkommer/förändringar görs.
Informationen finns även på vår hemsida.
Dokumentet uppdaterades 20250812

Inledning/Allmänt om GDPR (General Data Protection Regulation)
Dataskyddsförordningen är framförallt till för att skydda den registrerade (i vårt fall elever, vårdnadshavare och personal) så att inte personuppgifter hanteras på ett felaktigt sätt och kanske läcker ut eller finns kvar i våra arkiv och externa företags arkiv, helt utan syfte.
Lagen började gälla den 25 maj 2018 och är överordnad skollagen vad gäller persondataskydd.
Som skola måste vi hantera personuppgifter, annars kan vi inte bedriva verksamhet. Vi har dessutom en hel del krav på oss vad gäller att dokumentera och administrera data, som innehåller personuppgifter.

Vissa saker kan vara känsliga men mycket är vanliga listor/skolarbeten med namn eller foton. De är dock personuppgifter och vi måste ha **ett syfte** med att **lagra** dem, veta vilka som har **tillgång** till dem och en plan för när/hur de ska **raderas**.
Vi har olika lagrings-system med olika säkerhetsnivåer, tex all känslig information finns bara på vår server och saker som rör elevhälsan finns bara i ett system som kräver flerstegsinloggning. Pärmar och analoga data ska finnas på bestämda platser.

Vi använder externa företag och då måste vi ha ett **avtal** (personuppgiftsbiträdesavtal) med dem som säkerhetsställer att de hanterar våra personuppgifter på rätt sätt.

Som registrerad har man enligt den nya lagen **rätt till att få information om vad som lagras och hur det hanteras**, likaså rätten att bli raderad/bortglömd. Det sistnämnda kan vi endast tillgodose i vissa fall då vi som skola måste hantera personuppgifter/data för att kunna bedriva en fungerande verksamhet utifrån skollagen. När eleven är inskriven hos oss måste vi registrera personuppgifter helt enkelt.

Vad är en personuppgift
Vi på Tryde friskola måste enligt lagen ha full kontroll på var och hur data hanteras, lagras och raderas. Innehåller dessutom dokumentet någon form av en personuppgift så har vi en registerförteckning där vi registrerar vilken data vi lagrar och var den finns.
En personuppgift är något som kan leda fram till att en person kan identifieras. Det är t ex namn och inloggningsuppgifter men även en bild/foto där det går att utläsa vilken personen är (det räcker faktiskt tex med en hand, som har något märke som gör att man kan lista ut vem det är). Hit räknas även datorns IP-adress (enhetens unika nummer som går att spåra på internet) och en email-adress. Även det som lagras i elevernas (4-6) iPads och vårt styrprogram där man t ex kan se var den finns, och vilka program som används. Vissa personuppgifter är känsliga och måste hanteras efter särskilda regler. Tex så är elevens personnummer en sådan uppgift och måste skyddas bättre än standarddata.

Skolsjuksköterskan har behörigheter för att registrera uppgifter kring hälsa, för andra är det inte tillåtet. Det sker i ett extra säkert/skyddat system. I sjukanmälans-sms till oss ska ni endast ange ”frånvaro” och ej gå in på sjukdoms-detaljer, så att vi inte råkar få sådana register hos oss. Vi har policys för att radera sms (se stycket om hur vi hanterar data/personuppgifter). Information om frånvara-sms finns att läsa i utskicket ”skolstarts-info”.

Vad är samtycke

För att bedriva en skola, så måste vi hantera personuppgifter. Lagen säger att vi ska begära in samtycke (fritt översatt: ”godkännande”) för att vi ska få registrera uppgifter. Det är dock en omöjlighet då vi för massor av vanliga listor med deras namn och klass, tex gruppindelningar. Personuppgifter förekommer på alla arbeten som sen sätts in i elev-pärmar eller i deras lådor osv.
Därför tar skolor, i nuläget, inte in samtycke för den dagliga och nödvändiga verksamheten.
Vi **skickar ut samtyckes-förfrågan när det gäller hantering/lagring/gallring/radering** av personuppgifter. En blankett ges ut till alla nya familjer på skolan, där alla nuvarande tjänster finns med. Där får man ge samtycke till dessa tjänster. Man kan när som helst återkalla samtycket.
Blanketten finns på hemsidan som man kan skriva ut, fylla i och lämna in.
På blanketten ska det framgå i vilket syfte samt vilka uppgifter datan/tjänsten innehåller och när den raderas.
Är eleven under 13 år ska samtycket ske via vårdnadshavare. Då vi nästan endast har elever under 13 år så har vi som policy att **alltid hantera samtycke via vårdnadshavare.**

Fotografering

Privat fotografering är inte tillåtet. Foto är en personuppgift och regleras av GDPR, och det är vårt ansvar att ha kontroll på den datan. Massmedia kan dock kringgå det via något de kallar mingelbilder. När de är här så frågar de oss om det är okey, och sedan även eleverna individuellt.
Personalen har policys för hur vi får hantera/radera bilder, så att det uppfyller GDPR. *Vi tar till exempel endast foton med enheter som styrs av vår organisation, så att spridning inte kan ske.*

Rätten att bli bortglömd

I GDPR är en av huvudpelarna att man som person har rätt att bli bortglömd, dvs att alla data anonymiseras eller raderas.
Det är en omöjlighet för en skola då personuppgifter och data måste hanteras för att vi ska ha en fungerande verksamhet.

Personuppgiftsbiträdesavtal

Vi har tjänster som vi köper av andra företag, där data och personuppgifter hanteras.
Vi tecknar personuppgiftsbiträdesavtal med dem, som reglerar hur data hanteras och vår rätt att bestämma att data raderas osv. Det är viktigt tex när elever slutar hos oss. Då måste vi äga rätten att radera data/konto/personuppgifter s att de inte finns kvar i deras servrar (oftast online/molnbaserat).
Vi har avtal med nästan alla företag, framför allt alla de viktiga där mycket data och känslig data hanteras. Vi jobbar kontinuerligt med att få fler avtal på plats.

Dessa tjänster använder vi och har personuppgiftsbiträdesavtal med:

Teleservice (server, datorer, backuper, webbhotell till vår hemsida)
Prorenata (elevhälsan, utredningar, skolsjuksköterska)
Ne.se (uppslagsverk, UR-filmer, tema för alla ämne, kartor, appar)
mailadress, namn, födelseår, klass och aktivitet
Sanoma (läromedelsföretag, onlineläromedel, spel)
mailadress, namn, födelseår, klass och aktivitet
SLI education (utbildningsfilmer och radio)
Hantering regleras via deras sekretesspolicy.
Elevkonto raderas när elev slutar på skolan.
AV Media Skåne (pedagogiska tjänster)
mailadress, namn, födelseår, klass och aktivitet
Skolplus (pedagogiska digitala spel)
mailadress, namn, födelseår, klass och aktivitet
Inläsningstjänst och Polylino (digitalt bibliotek med inlästa läromedel)
mailadress, namn, födelseår, klass och aktivitet
Hi3G (mobil växel och mobiltelefoner)
sms, röstbrevlåda och samtalsloggar (telefonnummer och tid).

Infomentor (lärplattform med alla elever/klasser, schema osv. Interna dokument kring eleven sparas i tjänsten)

Övriga tjänster med personuppgiftsbehandling:

M365 (Copilot365) - Word, PowerPoint, Teams, Outlook osv
Det regleras via Microsoft Online Services Terms (OST) som uppdateras kontinuerligt och följer GDPR.
IT-ansvarig raderar personuppgifterna när elev slutar.
http://sli.se/service/integritetspolicy/ (elev kommer åt det inloggad)
JAMF och **JAMF Safe Internet** (DPA, Styrprogram för iPads)
Apple School Manager (elevkonton, Apple-ID,för att använda appar och iPad)
Det regleras genom att godkänna deras användarvillkor.

Hantering av data/personuppgifter

Personalen har olika scenarier vad gäller hur vi hanterar data. Extra viktigt är när det är känsliga personuppgifter och såklart data av sekretesskaraktär. Det heter klassning och leder till olika nivåer av säkerhet när det gäller att skydda data.

Elevhälsan använder sig av ett system som heter **Prorenata**, där det är tvåstegsinloggning och all data där skyddas extra mycket. Det är endast elevhälsan som har tillgång till tjänsten. All aktivitet loggas. Där finns många av våra sekretessdokument. Det används även av Tomelilla Kommun vilket gör det enkelt och säkert att skicka vidare dokument/data den dagen en elev börjar högstadiet.
Skolsjuksköterskan har en egen inloggning i Prorenata som bara hon kommer åt, där data kring hälsa hanteras.

Personal har tillgång till vissa sekretess-uppgifter via vår server (som sköts av **Teleservice**). Vi har tvåstegsinloggning där med och tillgången till datan är kraftigt begränsad och styrd av IT-ansvarig, så att personal endast kommer åt info den är direkt berörd av.

Personal och elever använder **M365** för utbildning som vår grund i allt praktiskt arbete. Det är en molntjänst och vi sparar aldrig sekretess eller känslig data där.
Vårt avtal med Microsoft gör att vi äger all data inom Office365, vilket betyder att de inte har någon insyn eller spårar det personal/elever gör där. Raderas data/konto så kan vi vara säkra på att all data är raderad och inte finns lagrad hos Microsoft.
Vi har tydliga policys för hur vår **mail** (ingår i Office365) ska hanteras. Om Ni mailar personal och där skriver känslig/sekretess information om ert barn, så har ni per automatik samtyckt till att den informationen hamnar i vår mailtjänst (molnbaserad). Vi raderar mail skyndsamt efter avslutat ärende. Data kan dock ligga kvar i Microsofts servrar vilket är utom vår kontroll. Personalen använder aldrig mail för känsliga ärenden.

Vid eventuell **SMS-kontakt** med skolan, så lämna inga känsliga uppgifter eller hälsotillstånd. Behöver Ni lämna mer info får Ni ringa till skolan/mentorn.

Vi har interna policys för våra **mobiltelefoner**. Data töms regelbundet, tex samtalsloggar och sms. Sms/röstbrevlådan/senaste samtal raderas skyndsamt efter avslutat ärende. Vi kan komma att spara namn och telefonnummer som en kontakt i våra telefoner, men de ses över regelbundet och raderas när det inte finns något syfte med att ha uppgifterna längre.
Vi har **låsbara skåp i klassrummet** där data av känslig/sekretess-karaktär ska vara. Organisationen har större **säkerhetsskåp** där data av känslig/sekretess-karaktär bevaras. Vi har riktlinjer för vad och hur det ska hanteras.

iPads
Elever i F-3 delar på iPads medan eleverna i 4-6 lånar en egen. De är DEP:ade och styrs via MDM. Det betyder att Apple har släppt ägandet till oss och vi styr helt över dem utan att de har någon insyn/rättighet alls.
I styrprogrammet för detta kan vi konfigurera hur vi vill att Ipaden ska fungera, vilka appar som ska finnas, vilka inställningar som är låsta osv.
Där är även ett antal funktioner som är mer kopplade till lagring av personuppgifter.
Det är endast IT-ansvarig på skolan som har tillgång till styrprogrammet.

Tex är där en funktion som på ett ungefär visar var iPaden befinner sig. Vilket är bra om den tex försvinner/tappas bort. Det går inte att radera internethistoriken, allt lagras i iPaden. Vi gör slumpmässiga stickprov för att kontrollera att det inte görs besök på olämpliga sidor och att Safari (webbläsaren) används till skolarbete. Det kan även vara elever med särskilda behov som har appar som är specifika för att träna vissa förmågor. Det kan man utläsa i styrprogrammet, vilka appar som finns hos en specifik elev. IT-ansvarig kan se många andra saker via styrprogrammet, tex vilka appar eleven använder mest, batteritid osv, men det är uppgifter som är av en mer okänslig karaktär.

När en elev slutar så tas användarnamnet/Apple-id/M365 genast bort och man kan inte längre spåra datan till en viss elev.
Vi har också som policy att alltid ominstallera som ny iPad när iPaden ska lånas ut igen till en annan elev.

Om vi skulle behöva använda oss av appar/tjänster/program (ej från företag vi har avtal med) där man måste ange personuppgifter på eleverna (namn, klass osv) så använder vi oss av figurerade uppgifter (pedagogen bestämmer) så att det blir anonymiserat och inga personuppgifter som går att knyta till en person.

Syfte
Vi måste alltid ha ett syfte med att hantera data/personuppgifter. Vi får inte ta med onödiga data/personuppgifter och när syftet är uppnått ska det raderas.
Denna tydliga policy gör att vi inte får gamla dokument liggandes (både digitalt och analogt) och alla ska känna sig trygga med att personuppgifter gallras/raderas när det inte längre behövs.
Vi får inte heller ändra att syfte i efterhand eller ändra syftet under arbetets gång.

Gör vi t ex en lista med elevernas namn och telefonnummer för att ha med oss till badet, så får vi inte använda den listan i ett annat syfte. Den får bara innehålla nödvändiga uppgifter för att uppfylla syftet och den ska raderas efteråt.

Radera data
En av våra viktigaste uppgifter inom skydd av personuppgifter/data är att se till att vi äger möjligheten att radera data. Om en elev slutar ska vi kunna se över (mha registerförteckningen) var personuppgifter finns lagrade och **skyndsamt radera dem**. Då gäller det att vi äger den möjligheten. Det regleras i personuppgiftsbiträdesavtalet (och deras integritetspolicys) när det är externa tjänster.

Det finns saker som vi har lagkrav på oss att bevara en längre tid, även om elev slutar. Det är till exempel betygskatalogen.

Vi har en möjlighet att **anonymisera data/dokument/IT-tjänster**, i stället för att radera, genom att ta bort all data som kan kopplas till en person (personuppgifter). Då kan vi spara datan/dokumenten hur länge som helst.

Vi använder oss alltid av **dokumentförstörare** för att säkra att dokument av känslig- eller sekretesskaraktär raderas och inte kan användas/identifieras.

Facebook och Instagram
Vi använder oss i nuläget av dessa tjänster som en kanal ut till vårdnadshavare, och när tjänsterna startas så måste deras villkor godkännas. Tyvärr är det så att de har sina servrar i USA och kan därför kringgå den nya GDPR som vi är skyldiga att följa. I villkoren framför det att de äger bilderna, så fast vi raderar dem så finns de kvar i deras servrar och kan när som helst användas av dem i till exempel marknadsföringssyfte, eller för att kartlägga/analysera. Det finns även kvar om andra personer i flödet delat inlägget. När det gäller Facebook så tillåter vi inte *(Vi har kvar kommentarsmöjligheterna tills vidare. Det är juridiskt utom vår kontroll.)* att utomstående fotar och i text anger personuppgifter, genom att kommentera något av våra inlägg.
Vi har inga personuppgifter på Instagram och vad gäller Facebook så regleras det via samtyckesblanketten.
Vi kan länka till vår hemsida där bilder på elever/verksamheten kan finnas, men då ligger bilderna hos oss och vi kan då radera den när vi vill, och den finns då inte alls hos Facebooks servrar.

Administration
Vi har externa molntjänster för vår administration, tex fritidsschema (IST) och faktureringsprogram. Där lagras personuppgifter. Genom att ni skapar konto där godkänner ni att Tomelilla kommun har tillgång till de personuppgifter/uppgifter ni anger där. Kontakta Tomelilla kommun om ni vill veta mer om hur de hanterar sin data.

Vill Ni veta mer föreslår vi:
https://www.imy.se/ (Integritetsskyddsmyndigheten)

Har Ni frågor är ni välkomna att kontakta:
Fredrik Larsson, IT-ansvarig
0417-14771 (anknytning 7)
fredrik.larsson@trydefriskola.se