Svenska kyrkan
BROMMA FÖRSAMLING

Regelverk för IT- och telefonianvändning
Antaget av KR 2020-01-28, med föreliggande reviderad version per 2021-01-28

Detta reglemente skall tas upp i Kyrkorådet för justering vid behov; en översyn bör ske minst en gång per mandatperiod.

Inledning
Detta regelverk, med tillhörande bilagor kompletterar Kyrkoordningen (KO) och gäller endast om den inte strider mot densamma.

Det har också tagits fram för att klargöra hur församlingen skall ha ett bra inbyggt dataskydd enligt dataskyddsförordningen.

Bromma församlings datorer, surfplattor och (mobil)telefoner – inkl. därmed använd kommunikation (e-post, sms m.m.) – är viktiga arbetsredskap (”verktyg”) för församlingens verksamhetsarbete.

Bestämmelserna i detta regelverk gäller församlingens anställda medarbetare, men även – i tillämpliga delar – *alla* som har tjänste-e-postkonto och/eller tillgång till församlingens ”smarta telefoner”/datorer/surfplattor och/eller församlingens trådlösa nätverk; uppdragstagare, ideella medarbetare, besökare och andra.

§ 1. Syfte och mål
Syftet med detta regelverk är att de berörda (d.v.s. de som nyttjar församlingens IT- och telefoniverktyg; datorer, surfplattor och (mobil)telefoner m.m.), skall känna till gränserna för dess användning – oavsett huruvida verktyget är av fast eller bärbar karaktär – gällande ex.vis Internet, e-post, sms m.m.; den som använder församlingens verktyg, och/eller som tilldelas ett tjänste-e-postkonto av Svenska kyrkan, förbinder sig att följa detta regelverk.

Det åligger kanslichefen (Kc) att tillse, att varje anställd förses med detta regelverk, liksom det åligger IT- och telefoni-ansvarig att tillse, att även varje person (utanför personalstaten) med e-postkonto förses med detta regelverk.

§ 2. GDPR-analys vid upphandling
Innan ett IT-system upphandlas (se även församlingens upphandlingsreglemente) eller införskaffas på församlingens initiativ eller genom anslutning till nationell nivås system, skall en analys enligt dataskyddsförordningen göras. Denna skall säkerställa att det finns korrekta ”personuppgiftsbiträdesavtal” och ”inbördes arrangemang”. Om inköp/införskaffande avser system, som omfattas av reglerna om konsekvensbedömning[1], skall en sådan bedömning

[1] En förteckning över när en konsekvensbedömning skall göras återfinns här: Integritetsskyddsmyndigheten (imy.se)

göras. Ett sådant fall avser ex.vis system som har amerikanska leverantörer. Kvarstår högre risker för registrerade skall konsekvensbedömningen lyftas till kyrkorådet, som har att ta ställning till om samråd med Integritetsskyddsmyndigheten skall inledas.

Församlingen skall sträva efter att använda mallar som är kvalitetssäkrade av församlingen i detta arbete. Vid behov skall dataskyddsombudet konsulteras.

§ 3. IT- och telefoni-ansvarig
I Bromma församling skall en anställd utses av Kyrkoherden (Kh), att agera ”IT- och telefoni-ansvarig”.

Praktisk hantering utifrån gällande avtal med operatör avseende inköp av hårdvara, dess mjukvara och andra tillbehör samt vid behov utökning av antalet abonnemang, skall ske genom församlingens IT- och telefoni-ansvarige (efter att hantering enligt 2 § skett).

IT- och telefoni-ansvarig har skyldighet att löpande hålla sig uppdaterad vad gäller Svenska kyrkans regelverk angående e-postsystem och gemensamma IT-plattform (se bilagorna till detta regelverk).

§ 4. Generellt
Nedladdning av programvara är inte tillåtet utan godkännande av IT- och telefoni-ansvarig och/eller Kc. Undantagna härifrån är automatiska uppdateringar av redan installerad, godkänd programvara (via operativsystemets uppdateringsfunktion), liksom uppdatering av redan installerat virusskydd.

Den anställde förbinder sig, att vara aktsam om sina arbetsredskap och att delta i av arbetsgivaren påbjudna utbildningar om handhavande/användande, liksom andra relaterade ämnen; i syfte att kunna utnyttja de tekniska fördelarna med utrustningen.

Innehavare av församlingens egendom ansvarar för att ev. förlust – oavsett orsak eller typ av verktyg – av utrustning omedelbart anmäls enligt församlingens rutin för personuppgiftincidenter. Tillkommande arbete kan innefatta anmälan till nätoperatör (för att snarast kunna spärra arbetsredskapet), polis (vilket måste göras av den som drabbats av förlusten) och till församlingens IT- och telefoni-ansvarige, som omedelbart skall spärra ev. nätverkskort i verktyget.

Innehållet (i form av ex.vis programvara, ”appar” och (arbetsrelaterade) dokument och filer) i församlingens arbetsredskap, tillhör arbetsgivaren. Det är av vikt, att ingenting görs eller installeras på/i utrustningen, som inkräktar på dess primära syfte; att vara ett arbetsredskap i församlingsarbetet. När arbetet lämnas (även om man går över till annan del inom Svenska kyrkan) får inga dokument – t.ex. i form av word- eller excelfiler – eller e-postmeddelande som innehåller personuppgifter, relaterade till arbetet i Bromma församling, tas med.

Arbetsgivaren har rätt att kontrollera samtliga verktyg, som tillhör församlingen och som tas upp i detta regelverk.

För varje anställd/användare finns ett specifikt (begränsat) lagringsutrymme i hemkatalogen (under ”H:”), vilket innebär att den enskilde måste ”hålla efter” – d.v.s. med lämpliga intervaller göra utrensningar – sin dokument-/fillagring.

Beträffande dokument (ex.vis word- eller excelfiler) med personuppgifter, skall dessa gallras fortlöpande och enligt de rutiner som fastställts enligt Svenska kyrkans bestämmelser 2019:1 och i övriga fall, enligt internt fastställda rutiner till exempel i integritetsreglementet och dokumenthanteringsplanen.

Dokument som innehåller personuppgifter måste ha en laglig grund för att sparas. Om en anställd/användare känner sig osäker på om laglig grund finns, kan församlingens dataskyddsombud konsulteras.

§ 5. Allmän kommunikation och kommunikation via ”sociala medier”
Förutom församlingen i sig, företräder församlingen också Svenska kyrkan i all kommunikation; detta regelverk relaterar därför till Svenska kyrkans regelverk rörande den gemensamma internetanslutningen och e-postsystemet i Kyrknätet (bilaga 1) samt den gemensamma IT-plattformen (bilaga 2), vilka församlingen är skyldig att efterfölja.

Vid kommunikation (se även församlingens eget kommunikationsreglemente) genom s.k. sociala medier, som ”Facebook” och liknande, är det av vikt, att medarbetare följer de regler som finns i KO samt i sekretesslagen, där sekretess och tystnadsplikt regleras. Vidare skall reglerna i dataskyddsförordningen följas, vilket innebär att församlingen inte skall ”sponsra” inlägg och endast använda sociala medier utifrån ett journalistiskt ändamål. Användandet av privata Facebook-konton eller Facebook-grupper för församlingens ändamål är inte tillåtet.

Beträffande Facebook (som f.n. inte följer GDPR) ”profilerar” dessa på allt man skriver/”lägger upp” (även i det som finns i ”slutna grupper”), vilket får till konsekvens att ”journalistiskt ändamål” [2] – vilket i sig, per definition, innebär att man riktar det skrivna till allmänheten (vilket, per definition, omöjliggör ”slutna grupper”) är det enda som får användas enligt detta reglemente.[3]

I de fall en anställd nyttjar sociala medier (som ex.vis Facebook) rent privat, måste det tydligt framgå att inläggen inte görs i egenskap som anställd i församlingen – det får inte råda någon tvekan huruvida det är i egenskapen privatperson eller anställd man skriver inlägg som har koppling till församlingen eller dess olika verksamheter. Detta innebär att om en anställd yttrar sig om församlingens verksamhet i sitt eget konto, måste det tydligt framgå att det är privatpersonen, som gör dessa inlägg.

Församlingen skall inte själv inrätta, eller upprätthålla, grupper beskrivna i denna paragraf. Observera dock, att grupperingar, som har direkt relation till församlingsarbetet, och som

[2] Begreppet ”journalistiskt ändamål” definieras inte i dataskyddsförordningen, men finns beskrivet i rättspraxis, och innebär att man informerar, utövar kritik eller väcker debatt i samhällsfrågor, som är av betydelse för allmänheten.

[3] Facebook-konton kan, då det relaterar till församlingens verksamhet, således enbart tillåtas om inläggen skrivs med ett journalistiskt ändamål.

ev. själv finns på dylika ”sociala medier” – ex.vis körer, ungdomsgrupper m.fl. – måste följa reglerna/förhållningssätten beskrivna i de bägge två föregående styckena.[4]

När en anställd är i tjänst, men ej är tillgänglig, är denne skyldig att utnyttja någon av de funktioner till vidarekoppling, hänvisning, röstmeddelande etc., som erbjuds i de olika systemen. Detta gäller vid all typ av frånvaro.[5] Se även §§ 7 och 8.

Kommunikationsområdet, vilket finns mer preciserat i församlingens kommunikationspolicy, utvecklas ständigt och som på alla ”nya” områden uppstår efter hand någon form av ”vett och etikett”. Det följande är avsett att framhållas som några viktigare exempel, som skall följas:

- All kommunikation skall präglas av god ton och respekt för varje människas integritet
- Alla telefonanrop skall besvaras med församlingsnamn, förnamn och efternamn
- Innan man ”svarar alla” i ett e-brev, skall man bedöma behovet av det (även väsentligt utifrån dataskyddsförordningens krav om att ”uppgiftsminimera”)
- Det är inte tillåtet att skicka eller sprida kedjebrev eller rykten
- Vid hanterande av känsliga personuppgifter[6] via e-brev skall dessa vara krypterade (vilket intern e-post med Svenska Kyrkan-adresser är) eller informationen skickas med ordinarie postgång
- Det skall alltid övervägas om e-post verkligen är det bästa lagringsalternativet; företrädesvis skall andra system användas, till exempel samverkansrum.

§ 6. Internet

- Internet är ett arbetsverktyg och får för privat bruk bara användas i sådan omfattning, att det inte inkräktar på arbetsuppgifterna eller sker i strid med dataskyddsförordningens regler. Även vid ev. privat användning – via församlingens egendom – skall dock detta regelverk efterföljas.
- All dataanvändning registreras i en ”logg” omfattande arbetsdatorns IP-adress samt namn på besökt webbplats. Otillåten ”surfning” skall rapporteras till användarens chef.

[4] Notera således att om man önskar en Facebooksida för att hantera medlemsadministration och/eller informera medlemmarna, detta inte är tillåtet (p.g.a. att Facebook ”profilerar” sina sidor och inte följer GDPR).

[5] Det rekommenderas att använda Outlook-kalendern för hänvisning, eftersom det ger synergieffekter för organisationen och övriga anställda. Man kan också, för telefonen, använda funktionerna i teledistributörens ”molnbaserad” växellösningar. Vid särskild överenskommelse med närmaste chef (d.v.s. Kh eller Verksamhetschef) kan anknytning medflyttas till passningsställe.

[6] Personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, liksom behandling av genetiska uppgifter, biometriska uppgifter (som entydigt kan identifiera en fysisk person), uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning, utgör känsliga personuppgifter.

- Otillåten surfning är ex.vis att besöka spelwebbplatser eller internetsidor som hyllar extremism eller med kränkande, rasistiskt, pornografiskt eller annat olämpligt innehåll.[7]
- ”Råkar” en medarbetare få upp olämpligt innehåll från internet, skall detta omgående rapporteras till närmaste chef.
- Det är inte tillåtet att delta – varken i tjänsten eller ”privat” om det sker med/via församlingens egendom – i chattsamtal med okända personer under påhittat namn.

§ 7. E-post

- Bromma församlings officiella e-postadress är bromma.forsamling@svenskakyrkan.se. Denna brevlåda skall läsas varje arbetsdag av Kc, eller annan personal på pastorsexpeditionen, som Kc uppdrar detta till. E-posten skall besvaras kontinuerligt under arbetsdagen till avsändaren, i förekommande fall med uppgift om till vilken/vilka befattningshavare e-posten vidaresänts.
- Kyrkorådets officiella e-postadress är kyrkorad.brommaforsamling@svenskakyrkan.se. Denna brevlåda skall läsas varje arbetsdag av Kc, eller annan person på pastorsexpeditionen, som Kc uppdrar detta till. E-posten skall utan dröjsmål vidarebefordras till kyrkorådets ordförande, eller annan person i kyrkorådet, som ordförande uppdrar detta till.
- De anställda ansvarar för att läsa och besvara sin e-post; i normalfallet inom 24 h. Hänsyn till ledigheter och semester skall dock tas.[8]
- Tjänste-e-postadressen (oftast fornamn.efternamn@svenskakyrkan.se) är ett arbetsredskap (privat användning av tjänste-e-postadressen bör inte ske). Kommunikation med e-post, som gäller anställning eller uppdrag i anställningen, skall ske med denna e-postadress.[9]
- Alla anställda skall använda den av Kh fastställda autosignaturen. Denna skall också länka till församlingens integritetsreglemente på hemsidan, om en sådan finns publicerad.
- Vid användning av e-post skall medarbetare alltid tänka på att e-postmeddelanden är offentliga handlingar, vilka skall diarieföras. Tänk också på att e-post kan innebära att meddelanden lättare sprids vidare, vilket kan vara negativt för den personliga integriteten. E-post av själavårdande karaktär skall därför undvikas; se § 10.
- Medarbetare skall vara insatta i vilka e-postmeddelanden som skall diarieföras enligt kyrkoordningens bestämmelser; efter att ett e-postmeddelande diarieförts skall det också gallras ur e-postsystemet.
- All trafik av elektronisk post och internetanvändning på församlingens datorer går via

[7] Kh äger dock rätt meddela skriftligt undantag i specifika fall, vilket i förekommande fall skall diarieföras (orsaken till).

[8] Härvidlag är det givetvis viktigt, att, beroende på vem som är frånvarande och vilka uppgifter denne har, hänvisning till annan lämplig anställd i förekommande fall görs.

[9] Vid tillfälliga driftsstörningar kan ev. eventuella privata adresser användas, men i dessa fall skall tjänstebrevlådans e-postadress anges i e-brevet.

”Kyrknätet”, vilket innebär att regler som gäller Kyrknätet/GIP (Svenska kyrkans Gemensamma IT-plattform) också gäller datoranvändningen i Bromma församling. Se bilaga 2.

- Storleken på minnesutrymmet i den egna e-postbrevlådan är begränsad. E-postkontot får därför inte användas som ”allmänt” lagringsutrymme, vilket också är direkt olämpligt utifrån dataskyddsförordningen. När gränsen för minnesutrymmet är nådd, kommer den enskilde inte att kunna sända och ta emot e-post. Det är därför viktigt, att den enskilde löpande efterhåller sitt e-postkonto (och raderar – eller flyttar till annat lagringsställ – brev, som inte kräver någon åtgärd och/eller som inte skall diarieföras).[10]
- Om e-post lagras kan i vissa fall detta behöva tas med i behandlingsregistret, vilket innebär att medarbetare behöver förklara sin e-postanvändning för att registret skall bli korrekt. För att minimera detta skall så få e-brev som möjligt lagras; istället skall Kyrksam, samverkansrum eller diariet användas för lagring.

§ 8. Dokumenthantering

För att utesluta att personuppgifter kan hamna i myndigheters händer i länder utanför EU/ESS, skall inga personuppgifter sparas i ”molntjänster” (till exempel i tjänster från amerikanska leverantörer, som Microsoft[11]) eller skickas via e-brev, om det kan antas att personuppgifterna kan vara intressanta för amerikanska myndigheter eller dessa omfattas av sekretess utifrån kyrkoordningen eller offentlighets- och sekretesslagens bestämmelser utan att berörda dokument först är krypterade. Krypteringsnyckel får inte förvaras på sådant sätt att en amerikansk leverantör kan få tag i den och den skall innehålla minst tio tecken, som innefattar både siffor och andra tecken. En annan möjlighet är i stället att spara uppgifterna lokalt på den egna enheten.

Som påpekats ovan är det viktigt att inte i onödan spara dokument i Word-, Excel eller liknande format, om de innehåller personuppgifter. För att undvika onödigt sparande och sparande av dubbletter skall följande principer gälla:

- Handlingar som diarieförs skall efter att de diarieförts inte sparas på annat sätt.
- Hantering av ”grupper” och liknande administration skall i första hand göras i Kyrksam och inte i egna Excel- eller Worddokument.
- För att undvika dubbellagring skall, när flera medarbetare samarbetar, samverkansrum användas. Dessa ska gallras fortlöpande och minst en gång per år.

§ 9. Mobil- och modemtelefoni

[10] Äldre uppgifter i e-postsystemen kan arkiveras på serverkonto eller hårddisk; med äldre uppgifter avses i första hand e-brev äldre än tolv månader.

[11] Någon annan leverantör av ”molntjänster” (än Microsoft), från leverantörer utanför EU/EES, får inte nyttjas; specifikt gällande Microsoft skall (när det används) det som anges ovan iakttas, d.v.s. bland annat att sekretessmässigt material, som innehåller personuppgifter, inte får lagras i sådan molntjänst utan kryptering.

- Alla anställda skall ha aktiverat sin röstbrevlåda så att inringande personer erbjuds lämna meddelande om medarbetare inte kan svara. Röstbrevlådan skall ha ett personligt meddelande, som innehåller organisation och namn på innehavaren.
- För att minimera risken för att andra olovandes skall kunna ta del av information, skall mobiltelefoner alltid vara inställda med automatiskt tangentlås kombinerat med ett lösenord. Lösenordet skall utformas så att det inte enkelt kan dechiffreras (bör innehålla både bokstäver och siffror och inte vara direkt kopplat till ens egen person eller familj).
- I förekommande fall skall ”platstjänster” vara aktiverade på varje mobiltelefon, liksom ”hitta min telefon”.
- Införskaffande av ”mobilappar” – oavsett om dessa är gratis eller kostar pengar – är företrädesvis inte tillåtet att göra för den enskilde (d.v.s. inte heller om ev. kostnad bestrids av den enskilde),[12] utan skall i förekommande fall hanteras/godkännas av Kh eller annan verksamhetschef.
- Telefon – inkl. telefonmodem i datorer/motsvarande – får ej användas utomlands, utan godkännande från Kh. Detsamma gäller i förekommande fall vid önskemål om att ringa utlandssamtal från Sverige. Observera att lokala ”WiFi-nät” inte får användas för datatrafik. Det enda WiFi-nät som får nyttjas är Svenska kyrkans egna (som ligger innanför Svenska kyrkans ”brandvägg”).
- Vid resor eller överföringar (till exempel e-post) till länder utanför EU/EES tillkommer att en ordentlig riskbedömning (utöver föregående punkt) behöver göras. Detta innebär att Kh i dessa fall behöver fatta ett särskilt beslut i frågan, där de villkor som gäller är tydliga. Dataskyddsombudet bör också tillfrågas innan beslut fattas.
- Den anställde skall, i det fall man innehar en s.k. ”smart telefon”, aktivera e-post och kalender i telefonen. Detta innebär, att man med sin telefon också har att följa gällande regelverk för e-post och internetanvändning; se §§ 6 och 7.

§ 10. Privat bruk

- Medarbetarna har, i skälig omfattning, rätt att använda arbetsdatorerna för privat bruk (utanför ordinarie arbetstid) så länge den användningen inte innefattar personuppgiftsbehandling. Dock under samma regler, som framgår i detta reglemente, i övrigt.
- Beträffande det omvända – d.v.s. att använda kommunikationsverktyg som inte är inköpta av församlingen, till arbetsrelaterade uppgifter – måste individen[13] nyttja ”stor försiktighet” (eftersom det finns en uppenbar risk för att ett ”privat” verktyg (ex.vis en mobiltelefon) inte har samma säkerhet som församlingens verktyg).
- Skulle privata verktyg användas för församlingsändamål, får dock inte dokument – inkl. e-brev – lagras i dessa (ex.vis hårddiskar, egna ”molntjänster” eller ”lokalt” i

[12] Detta gäller exempelvis spel, som dels tar stor lagringsplats, dels vars ”surf” hamnar på församlingens teleoperatörsfaktura.

[13] Torde i första hand gälla volontärer och förtroendevalda.

mobiltelefoner).

- Utskrifter och kopiering som medarbetare gör från datorer – och som relaterar till privat användning – är som regel ej tillåten.
- Privata telefonsamtal skall under arbetstid, om möjligt, undvikas.

§ 11. Själavård
Enligt KO gäller förbud mot att röja sådana uppgifter, som har anförtrotts en biskop eller präst under bikt eller enskild själavård. Förbud gäller också mot att röja sådana uppgifter, som har anförtrotts en diakon under själavårdande samtal. Enligt KO skall denna typ av handlingar därför inte diarieföras.

I Biskopsbrevet "Tystnadsplikt och sekretess 2000" (senast reviderad 2004)[14] anges: "För att kunna leva upp till sitt ansvar är det angeläget att varje präst har en tydlig ordning för hanteringen av brev som skall skyddas av tystnadsplikt. De brev som ligger under tystnadsplikt får inte komma till någon annans kännedom och bör därför förstöras."

Detta gäller även e-post. Detta innebär, att datorer i princip aldrig skall innehålla handlingar som rör bikt eller avser enskild själavård.

§ 12. Kontroll
Arbetsgivaren har rätt att – vid ex.vis misstanke om felaktig hantering, virusangrepp eller felaktigheter enligt dataskyddsförordningen – gå igenom e-post och datorhistorik i medarbetarnas arbetsredskap (gäller inte dataskyddsombudet), inkl. telefoner, som ägs av församlingen. Även i de fall en registrerad individ begär ett registerutdrag, äger arbetsgivaren rätt att gå igenom e-postkonton (i syfte att skapa ett korrekt registerutdrag). Även för att skapa ett korrekt behandlingsregister, har arbetsgivaren rätt att gå igenom lagring som sker i olika arbetsredskap.

Om dataskyddsombudets utrustning behöver gås igenom skall det ske med samtycke från denne, eftersom ombudet kan ha tystnadsplikt för uppgifter, som hör till det uppdraget.

Beslut om ev. kontroll fattas av Kh efter hörande av IT- och telefoni-ansvarig.

Vid misstanke om rena lagbrott, skall församlingen göra en polisanmälan.

§ 13. Regelverkets efterlevnad
En anställd, förtroendevald eller frivillig, som bryter mot reglerna i detta regelverk, kan komma att bli föremål för disciplinära beslut. Inför sådana beslut skall arbetsgivaren göra en noggrann utredning.

Om en användare misstänks för brott eller om enhetens utrustning varit föremål för brott eller använts som brottsverktyg vid exempelvis förtal, pornografibrott, dataintrång, förskingring och bedrägeri, skall polisanmälan göras.

[14] Biskopsbrevet Tystnadsplikt och sekretess finns på svenskakyrkan.se/arkebiskopen/6.htm#Biskopsbrev

Hanteringen av personuppgifter i en polisanmälan skall i sig ske med varsamhet och i enlighet med Kh:s anvisningar. Dataskyddsombudet kan här behöva konsulteras.

Sammanställning över bilagor till detta regelverk

Bilaga 1: Policy för användning av Svenska kyrkans gemensamma Internetanslutning och e-postsystem i Kyrknätet (beslutad av Svenska kyrkans IT-ledning 2007-06-20)

Bilaga 2: Policy för Svenska kyrkans gemensamma IT-plattform (beslutad av Svenska kyrkans IT-ledning 2010-06-24)