Col·legi
Mare de Déu del Carme
Pares Carmelites

REGLAMENT SOBRE UTILITZACIÓ DELS RECURSOS DE LES TECNOLOGIES DE LA INFORMACIÓ I LA COMUNICACIÓ (TIC)

ÍNDEX

1.- **Disposicions generals**.

En data **9 de juny de 2022** es va aprovar el Codi de Conducta que estableix com un dels principis d'actuació ***«Ús adequat de les eines informàtiques»***.

L'absoluta rellevància que ha tingut la irrupció de les noves tecnologies en el desenvolupament de l'activitat i comunicació de l'organització/comunitat educativa, comporta la necessitat d'adoptar les mesures adequades per a la seva utilització correcta, tot això per garantir la protecció de tots els béns jurídics que estan en joc.

2.- **Objecte**.

L'objecte del present Reglament és definir de manera clara, quin ha de ser l'ús que cal donar a les TIC (Tecnologies d'Informació i Comunicació) corporatives. Aquest protocol es troba en sincronització amb les condicions generals de cessió di portàtils que té incorporada l'organització als docents, en especial quant a l'ús privat dels mateixos.

3.- **Definició de Tecnologies de la Informació i la Comunicació** (TIC).

Les Tecnologies de la Informació i la Comunicació (TIC) són el conjunt d'eines, aplicacions i instruments desenvolupats per gestionar informació i enviar-la d'un lloc a l'altre. Inclouen les tecnologies per emmagatzemar informació i recuperar-la després, així com per enviar-la d'un lloc a un altre i/o processar aquesta informació.

D'aquesta manera, les **TIC** conformen el conjunt de recursos necessaris per tractar informació a través d'ordinadors, dispositius electrònics, aplicacions informàtiques i xarxes socials, necessàries totes per emmagatzemar-la, convertir-la, administrar-la i transmetre-la, permetent un millor accés i classificació de la informació per al desenvolupament de la seva activitat organització/comunitat educativa.

4.- **Principi de confidencialitat**.

La confidencialitat de les comunicacions constitueix un dret fonamental reconegut a la Constitució Espanyola, que ha de guiar la manera de rebre i proporcionar la informació.

L'organització/comunitat educativa i els treballadors integraran en el seu desenvolupament professional i personal la protecció de la totalitat de les dades de què tinguin coneixement per la seva relació laboral amb COL·LEGI MARE DE DÉU DEL CARME, procurant-ne la gestió adequada i responsable.

Dins l'àmbit del principi de la confidencialitat, ens referirem a tres àmbits:

- Els establerts per la **Llei de protecció de dades**.
    - Es garantirà que les dades que poguessin recollir, obtenir, o conèixer, per la seva feina, ia través de qualsevol canal -web, xarxes socials, bloc, oficines del client, etc…-, no es podran transferir a tercers sota cap concepte, ni s'utilitzaran per a ús personal.
- Els que determini la **estratègia de l'organització/comunitat educativa**: la informació que ha de ser coneguda únicament per determinats grups de persones, per maximitzar la possibilitat d'èxit de les decisions preses.
- S'establiran dins de l'estructura de l'organització/comunitat educativa, els administradors de sistema, que es renovaran anualment i que seran els únics amb accés a aquest sistema. Qualsevol autorització d'administrador a altres membres de l'organització/comunitat educativa s'haurà de documentar per escrit, indicant-ne l'objecte de l'accés i la durada.
- **Acords de confidencialitat** amb tercers (clients, proveïdors, assessors, etc…).

La confidencialitat és un element transversal a tenir en compte a les comunicacions de la totalitat dels membres de l'organització/comunitat educativa.

L'accés a les comunicacions dels membres de l'organització/comunitat educativa es farà sota la més estricta legalitat constitucionalitat, protegint-ne la intimitat, l'honor i la pròpia imatge.

En el marc del principi de confidencialitat s'estableix l'obligació, per a tots els membres de l'organització/comunitat educativa, de no confeccionar còpies o duplicats de la informació confidencial a què pugui tenir accés cadascun.

La recepció d'informació confidencial es posarà en coneixement de l'organització/comunitat educativa a través dels mecanismes previstos en l'organització/comunitat educativa, amb celeritat i immediatesa.

5.- **Dret d'informació de la política organització/comunitat educativa al personal de l'organització/comunitat educativa**.

L'organització/comunitat educativa haurà d'informar de les normes d'utilització de les TIC, de manera clara, transparent i constant, com a forma d'implantar una consciència transversal en el seu ús, i amb la finalitat de generar una cultura d'acord amb les exigències constants en aquest àmbit.

L'organització/comunitat educativa desenvoluparà la formació necessària que minimitzi els possibles riscos en l'ús de les eines esmentades.

En aquesta política que, queda definida en aquest Reglament, es fixarà per als membres de l'organització/comunitat educativa un deure de formació, així com la possibilitat per part de l'ocupador, de la direcció i control de l'activitat laboral, de la qual es determinarà de forma expressa la manera i l'abast per evitar una minva en la privadesa del treballador.

6.- **Deure formació en política organització/comunitat educativa de les TIC'S.**

L´organització/comunitat educativa es compromet a desenvolupar una formació adequada, ajustada i reiterada de les TICS als membres de l'organització/comunitat educativa.

Per això, s'establirà a les plataformes internes existents per a tots els empleats amb COL·LEGI MARE DE DÉU DEL CARME, el recordatori del Document de Seguretat i els seus sistemes d'accés.

7.- **Direcció i control de l'activitat laboral.**

7.1.- ***Interval***.

Cada vegada és més evident la revolució tecnològica que ha portat a la utilització de les noves tecnologies per a la major part del desenvolupament de la vida social, familiar, i també per descomptat, de l'entorn laboral, cosa que comporta la possibilitat i/o necessitat que els treballadors comptin amb eines informàtiques per al desenvolupament de la seva feina habitual.

Però la privadesa del treballador "*s'ha de conciliar amb altres drets i interessos legítims de l'ocupador, en particular, el dret a administrar amb certa eficàcia l'organització/comunitat educativa, i sobretot, el dret a protegir-se de la responsabilitat o el perjudici que es pugui derivar de les accions dels treballadors*"[1].

S'estableix en aquest reglament com es durà a terme aquesta vigilància i control per verificar el compliment, per part del treballador, de les seves obligacions i deures laborals, salvaguardant, en la seva adopció, els drets d'aquells.

7.2.- ***Vigilància i control dels mitjans productius corporatius***.

Els mitjans productius de l'organització/comunitat educativa corresponen a l'organització/comunitat educativa i, en cap cas, no es poden considerar propietat dels seus empleats.

L'organització/comunitat educativa podrà adoptar les mesures que consideri més oportunes per a la vigilància i control del compliment, per part del treballador, de les seves obligacions i deures tasques, tal com assenyala el particular de la Sentència del Tribunal Suprem -Sala Social- de 26 de setembre de 2007:

---

[1] Grup de treball "Article 29": grup consultiu independent encarregat d'estudiar qüestions relatives a l'aplicació de les mesures nacionals adoptades en virtut de la Directiva 679/16.

Tant la persona del treballador, com els efectes personals i la taquilla formen part de l'esfera privada d'aquell i queden fora de l'àmbit d'execució el contracte de treball a què s'estenen els poders de l'article 20 de l'Estatut dels treballadors. ***Per contra, les mesures de control sobre els mitjans informàtics posats a disposició dels treballadors es troben, en principi, dins de l'àmbit normal d'aquests poders: l'ordinador és un instrument de producció del qual és titular l'organització/comunitat educativa "com a propietari o per un altre títol" i aquest té, per tant, facultats de control de la utilització, que inclouen lògicament el seu examen***. D'altra banda, amb l'ordinador s'executa la prestació de treball i, en conseqüència, l'organització/comunitat educativa pot verificar-hi el compliment correcte, cosa que no succeeix en els supòsits de l'article 18, ja que fins i tot respecte a la taquilla, que és un bé moble de l'organització/comunitat educativa, hi ha una cessió d'ús a favor del treballador que en delimita una utilització per aquest que, encara que vincula poders organització/comunitat educativa de l'article 20 de l'Estatut dels Treballadors per entrar dins de lespera personal del treballador".

7.3.- ***Principis que han de regir aquesta activitat de vigilància i control***.

7.3.1.- Necessitat: L'ocupador, abans de procedir a l'activitat de vigilància i control, ha de comprovar si és absolutament necessària per a un objectiu específic.

Per tant, aquesta mesura tindrà caràcter excepcional. Algunes conductes que poden justificar el control del correu electrònic d'un treballador per obtenir informació o prova de determinats actes són:

- Investigació d'actuació presumptament delictiva d'un treballador, que obligués l'ocupador a defensar els seus interessos, i així podria ser declarat responsable civil subsidiari dels actes d'aquest treballador.
- Obertura de correu electrònic d'un treballador quan sigui necessari (per trobar-se de baixa per malaltia o de vacances) i no se n'hagi pogut derivar la correspondència a altres empleats (via funcions de resposta o desviació automàtica).
- Detecció de virus maliciosos que requereixin conèixer-ne l'origen i poder garantir la seguretat del sistema.

7.3.2.- Finalitat: Les dades s'hauran de recollir per a una finalitat

determinada i legítima, i aquestes dades no podran ser tractades posteriorment amb altres objectius.

Es considerarà un fi legítim, per exemple, evitar la fugida d'informació confidencial a un competidor.

7.3.3.- Transparència: L'ocupador comunicarà a tots els empleats la política de vigilància i control dels correus i informarà de manera completa sobre les circumstàncies que poden justificar aquesta mesura, l'abast i la seva aplicació, que haurà d'incloure necessàriament:

- Política d'utilització de correu electrònic i Internet per part dels empleats, així com en quina mesura pot ser utilitzada per a fins privats o personals.
- Quan hi hagi autorització per a ús de correu electrònic per a fins personals o privats, la vigilància i control sobre ells serà molt limitada (ex. quan es tracti de detectar entrada de virus i sigui necessari per garantir la seguretat del sistema).

7.3.4.- Proporcionalitat: S'exclou el control general dels missatges electrònics i de la utilització d'Internet per tot el personal, excepte quan sigui necessari per garantir la seguretat del sistema.

La tecnologia actual ofereix programes que permeten avaluar la utilització del correu electrònic per part de cadascun dels empleats, informant del nombre de missatges enviats i rebuts, així com de les dades o documents que s'hi adjunten.

D'altra banda, la tecnologia també ofereix sistemes de bloqueig adequats per evitar l'ús abusiu d'Internet, més enllà de l'autoritzat per l'ocupador.

7.4.- ***Control del correu electrònic***.

Aquest control s'ha de fixar sempre sota els principis indicats a l'apartat anterior, de manera que, quan sigui necessari, l'accés al correu electrònic s'ha de fer sota programes informàtics de cerca cega dirigida i no indiscriminada.

Aquesta revisió es realitzarà en presència del membre de l'organització/comunitat educativa al correu electrònic de la qual s'accedirà, o bé del seu representant sindical. A aquest efecte s'aixecarà la corresponent acta en què s'identifiqui les persones que intervinguin, amb indicació precisa de l'objecte d'aquest accés i del resultat.

S'autoritzarà per tots els membres de l'organització/comunitat educativa, la possibilitat d'accés i realització d'actuacions informàtiques de còpia -mitjançant bolcat- del correu professional

-corporatiu-.

A aquest efecte, es donarà a conèixer a tots els treballadors el **Annex 1** del present Reglament relatiu a **Polítiques d'utilització de les TIC.**

7.5.- ***Control de l'accés a Internet.***

Es permet un ús raonable de l'Internet per a fins personals i privats de forma excepcional.

Dins del límit del que és raonablement possible, la política de l'organització/comunitat educativa respecte a Internet es basarà més en la prevenció que en la detecció. En aquest sentit, es donarà prioritat a la utilització d'eines tècniques dirigides a limitar l'accés a determinades pàgines o descàrregues de determinats continguts -per exemple, mitjançant el bloqueig a algunes pàgines web o instal·lant advertiments automàtics-.

Es facilitarà informació ràpida al treballador quan es detecti la utilització sospitosa d'Internet per tal de minimitzar els problemes, no només d'un ús abusiu, sinó també de possibles riscos en la seguretat de la xarxa. En aquest sentit, amb la comprovació del temps emprat o l'elaboració d'una llista de les webs més visitades, n'hi ha prou per confirmar l'actuació correcta, o incorrecta, del treballador.

Si aquestes comprovacions generals revelessin una possible utilització abusiva d'Internet, l'ocupador podria aleshores valorar la possibilitat de procedir a determinats controls a la zona de risc.

En tot cas, s'informarà el treballador dels fets coneguts mitjançant aquestes eines, a fi que pugui refutar la utilització abusiva al·legada per l'ocupador.

En aquest sentit, s'informarà clarament els treballadors en quines condicions s'autoritza la utilització d'Internet amb finalitats privades, amb indicació expressa dels elements que no es puguin descarregar, copiar o visualitzar.

S'indicarà també al **Annex 1**, els sistemes instal·lats per impedir l'accés a determinats llocs o detectar-ne una possible utilització abusiva, així com si aquest es durà a terme de manera individualitzada o per departaments, i si el contingut de les webs consultades serà visualitzat o registrat per l'ocupador en determinats casos.

7.6.- ***Expectativa d'ús privatiu de mitjans productius corporatius***.

L'organització/comunitat educativa permet i autoritza una certa tolerància de l'ús de mitjans corporatius mitjançant les TICS per a ús personal i privat dels treballadors, sempre que tinguin relació directa amb el funcionament de l'organització/comunitat educativa. (Missatges sindicals…).

En el cas d'utilització per a fins exclusivament privats, aquest es durà a terme a través de compte de correu privat (WEB)- No serà possible utilitzar el correu electrònic corporatiu.

7.7.- ***Monitorització del correu electrònic i serveis d'accés a internet***.

S'estableix en aquest Reglament la possibilitat de monitorització per part de l'organització/comunitat educativa del correu electrònic corporatiu i serveis d'accés a Internet dels empleats, en els termes establerts en aquesta **Annex 1** d'aquest document.

ANNEX 1.- Política i normes d'utilització i control de les tecnologies de la informació i comunicacions (TIC) al COL.LEGI MARE DE DÉU DEL CARME

1.- **OBJECTIU**.

L'objectiu d'aquesta Política és establir les línies d'actuació que cal tenir en compte per tal de garantir l'ús responsable i adequat de les tecnologies de la informació i les comunicacions (d'ara endavant TIC) de l'organització/comunitat educativa COL·LEGI MARE DE DÉU DEL CARME, així com establir els sistemes de control i les conseqüències que l'incompliment d'aquesta política pugui comportar els seus empleats.

Aquesta política estarà integrada en el Codi Ètic i Conveni Col·lectiu, si n'hi hagués, aprovats al seu dia per a COL·LEGI MARE DE DÉU DEL CARME, així com amb la normativa en matèria de protecció de dades personals, a la qual també es fa referència en aquest document.

Aquesta política s'ha comunicat als representants dels treballadors i després serà comunicada a tots els empleats.

2.- **POLÍTICA D'ÚS I CONTROL DE LES TIC**.

2.1- **POLÍTICA D'ÚS DE LES TIC**

COL·LEGI MARE DE DÉU DEL CARME, és una organització/comunitat educativa conscienciada amb la importància que revesteix la protecció de dades personals i la seguretat dels sistemes d'informació. Per això, vol posar tots els mitjans necessaris per assolir un màxim nivell de seguretat, així com donar estricte compliment a la legalitat vigent. En conseqüència, posa de manifest que:

a) Els empleats que utilitzin els equips i recursos informàtics posats a la seva disposició per COL·LEGI MARE DE DÉU DEL CARME són responsables de la seva conservació, així com de la seva utilització d'acord amb la Llei i amb les regles establertes en aquest protocol. Aquests recursos i equips són propietat de COL·LEGI MARE DE DÉU DEL CARME, i només se'n permet la utilització per desenvolupar les tasques establertes en l'àmbit laboral.

b) L'organització/comunitat educativa únicament admet la utilització de les TICS i eines informàtiques per a ús personal i privat, de manera excepcional i quan això fos estrictament necessari.

c) Lús de les TICS serà controlat tant per motius de seguretat com per motius de control de lactivitat laboral. Pel que fa al sistema de control, es donarà prioritat a la utilització de ferramentes de prevenció i control menys

invasius ia través del mesurament de volum, trànsit, activitat, extensions d'arxius, etc…

d) Es podran establir sistemes de control basats en tasts aleatoris però que no suposin d'inici un control total de l'activitat.

e) Es podran adoptar les mesures legals oportunes davant de l'incompliment d'aquestes polítiques i normes i, en general, davant de l'incompliment de la legalitat vigent, del Codi Ètic o del Conveni Col·lectiu.

f) Les claus d'accés per accedir als sistemes i equips informàtics consten d'un nom d'usuari i contrasenya -password-, que són secrets, personals i intransferibles. Per això es prohibeix la seva comunicació a altres persones llevat que hi concorrin motius urgents i extraordinaris que justifiquin aquesta comunicació.

2.2. **NORMES D'ÚS**

Amb caràcter general, sempre es procurarà treballar sobre els servidors corporatius. Quan sigui necessari treballar en mode local, l'empleat serà responsable que la informació continguda a l'equip -siguin o no dades personals- quedi guardada degudament al servidor habilitat a aquest efecte per evitar-ne la pèrdua.

2.2.1.- **ÚS DEL CORREU ELECTRÒNIC CORPORATIU:**

a) El correu electrònic corporatiu es configura com una eina de treball.

b) L'ús del nom o els cognoms dels empleats al costat del domini de l'organització/comunitat educativa no significa l'assignació per l'organització/comunitat educativa d'un correu personal, sinó que aquest correu està vinculat a l'àrea i al lloc de treball.

c) Es podrà realitzar còpia de seguretat dels mails i accedir al seu contingut, davant de problemes tècnics o de seguretat o bé quan hi hagi sospites d'incompliment de les normes contingudes en aquest document.

d) El correu electrònic corporatiu no s'ha de fer servir com a eina de difusió de correus massius.

e) Es prohibeix expressament fer enviaments de missatges de forma massiva o en cadena, no autoritzats, especialment aquells amb

finalitats comercials o publicitàries sense el consentiment del destinatari (correu escombraries o spam).

f) Atès que el correu electrònic és una de les fonts més importants de difusió de virus, es recomana no obrir missatges rebuts de remitents desconeguts,

especialment si a més de desconeguts, tenen l'assumpte en anglès -a excepció d'aquells la llengua docent dels quals sigui aquesta- o porten arxius adjunts. S'eliminaran els missatges amb annexos susceptibles d'execució.

g) Es prohibeix qualsevol mena d'enviament sense relació amb l'activitat professional que pertorbi el funcionament normal de la xarxa.

h) Es prohibeix expressament l'ús no autoritzat de correu daltres companys així com la falsificació de missatges de correu electrònic, ja sigui sobre el seu contingut o manipulant les capçaleres per ocultar la identitat de l'usuari remitent.

2.2.2. **ACCÉS A INTERNET.**

a) L'accés a Internet es configura com una eina a disposició dels empleats per al compliment de les seves tasques i funcions a l'organització/comunitat educativa.

b) No es podran descarregar o utilitzar programes o programaris que no estiguin prèviament i expressament autoritzats per l'organització/comunitat educativa. Si és necessari, se sol·licitarà autorització al Director de Serveis Informàtics.

2.2.3 **DISPOSITIUS D'EMMAGATZEMATGE EXTERN.**

Els usuaris no utilitzaran dispositius d'emmagatzematge extern. Quan de manera excepcional sigui necessari, se sol·licitarà autorització per fer-ho al Director de Serveis Informàtics i s'adoptaran totes les mesures de seguretat:

- Quan se n'autoritzi l'ús, els dispositius seran sempre facilitats per l'organització/comunitat educativa.

- La informació continguda en aquests dispositius es desarà xifrada o amb contrasenya.

2.2.4.- **ALTRES CONDUCTES PROHIBIDES** (relatives tant a l'ús de correu electrònic, Internet i xarxes socials).

a) La utilització i el tractament de dades de caràcter personal de tercers sense l'autorització necessària.

b) L'enviament de missatges o imatges amb material ofensiu, inadequat o amb continguts discriminatoris per raó de gènere, així com aquells que promoguin l'assetjament sexual.

c) Utilitzar la xarxa per a jocs d'atzar, sorteigs, subhastes, descàrregues de vídeos, àudio o altres materials no relacionats amb l'activitat professional.

d) Alterar, destruir, inutilitzar o danyar de qualsevol manera les dades, programes o continguts electrònics de COL·LEGI MARE DE DÉU DEL CARME o de tercers.

Aquests actes poden constituir delicte de danys, que preveu l'article 264.2 del Codi Penal.

e) Introduir, descarregar d'Internet, reproduir, utilitzar o distribuir programes informàtics no autoritzats expressament per la direcció tècnica o altres tipus de materials protegits per drets de propietat intel·lectual, quan no es disposi d'autorització.

f) Instal·lar o executar des de qualsevol punt de la xarxa, programes o arxius via Internet oa través de qualsevol altre suport extern (USB, CD,…) sense autorització expressa del Director de Serveis Informàtics.

g) Instal·lar o executar des de qualsevol punt de la xarxa, programes o fitxers que tinguin per finalitat, o amb els quals s'intenti accedir, descobrir, manipular o destruir, informació diferent de la que correspongui a l'empleat, sigui quin sigui el mitjà emprat -detectors, escàners de ports, programes d'administració remota, …

h) Emprar identificadors i contrasenyes d'altres usuaris per accedir al sistema. Facilitar a altres empleats l'identificador i la contrasenya personal a altres empleats llevat dels casos expressament previstos i autoritzats.

i) Burlar les mesures de seguretat establertes pel sistema informàtic, per accedir a continguts -fitxers o programes- l'accés dels quals no li estigui permès.

j) Modificar la configuració de xarxes, equips i/o qualsevol dispositiu de treball.

k) Endur-se els equips o ordinadors personals als domicilis particulars, fins i tot quan sigui per fer tasques professionals, sense comptar amb l'autorització expressa (per escrit) del responsable d'Informàtica.

k) I, en general, emprar la xarxa corporativa, sistemes informàtics i qualsevol mitjà posat a l'abast de l'empleat, vulnerant el dret de tercers, els drets de la pròpia organització/comunitat educativa, o realitzar qualsevol altre acte que es pugui considerar il·lícit pel Codi Penal.

3.- **PROTECCIÓ DE DADES**

3.1.- **POLÍTICA RELATIVA A LA PROTECCIÓ DE DADES**

Per tal de garantir un tractament responsable i adequat de les dades

personals dels mateixos empleats i de tercers, i donar compliment a l'exigència legal de protegir tant els fitxers automatitzats com els no automatitzats, es detallen a continuació les obligacions generals relatives a la protecció de dades qualsevol que sigui el suport en què es trobin.

3.2.- **OBLIGACIONS GENERALS I COMUNS**-FITXERS AUTOMATITZATS I NO AUTOMATITZATS (PAPER).

a) Guardar la necessària reserva respecte a qualsevol tipus d'informació de caràcter personal coneguda en funció del treball desenvolupat, fins i tot un cop conclosa la relació laboral amb COL·LEGI MARE DE DÉU DEL CARME.

b) Guardar tots els suports físics i/o documents que continguin informació amb dades de caràcter personal en un lloc segur, quan aquests no estiguin sent utilitzats i, especialment, una vegada conclosa la jornada laboral.

c) Queda prohibit el trasllat per qualsevol mitjà -via correu electrònic mitjançant remissió de correus electrònics de l'ordinador de l'organització/comunitat educativa a l'ordinador personal, mitjançant copiat en dispositius d'emmagatzematge extern -CD, USB,...- de llistats, arxius o documents amb dades de caràcter personal en què es guardi informació titularitat de COL·LEGI MARE DE DÉU DEL CARME fora de Informàtics. En el supòsit de resultar necessari aquest trasllat o remissió de suport, arxiu o document, aquest es realitzarà xifrant les dades, o utilitzant mecanismes que dificultin l'accés o la manipulació per tercers en cas de pèrdua o robatori.

d) Els ***fitxers de caràcter temporal*** són aquells que emmagatzemen dades de caràcter personal per al compliment d'una necessitat determinada o treball temporal i quan la seva existència no sigui superior a un mes. Aquests fitxers han de ser esborrats una vegada deixin de ser necessaris i, mentre mantinguis la seva vigència, han de complir els nivells de seguretat assignats pel Responsable de Seguretat. Si transcorregut un mes, l'empleat requereix continuar utilitzant la informació emmagatzemada en aquest fitxer, ho ha de comunicar al responsable de seguretat a fi d'adoptar les mesures oportunes sobre el particular.

e) Només les persones autoritzades al llistat d'accessos podran introduir, modificar o anul·lar les dades contingudes als fitxers o documents objecte de protecció. Els permisos d'accessos dels empleats són concedits pel responsable de seguretat. Si algun empleat requereix per al desenvolupament de la seva feina accedir a fitxers o documents a l'accés dels quals no estigui autoritzat, ho comunicarà al responsable de seguretat corresponent perquè li faciliti aquest accés pel temps necessari.

f) Comunicar al Responsable de Seguretat, les possibles incidències de què pugui tenir coneixement qualsevol empleat.

3.3.- **OBLIGACIONS ESPECÍFIQUES PER ALS FITXERS AUTOMATITZATS**

a) Canviar les contrasenyes quan el sistema ho requereixi i guardar la reserva oportuna.

b) Tancar o bloquejar les sessions a la finalització de la jornada laboral o quan l'empleat s'absenti temporalment del lloc de treball, per evitar accessos no autoritzats.

c) No copiar informació de fitxers o documents en què s'emmagatzemin dades de caràcter personal a l'ordinador personal, sense autorització expressa del Responsable de Seguretat i sense adoptar les mesures de seguretat i custòdia per evitar l'accés per part de tercers.

d) Arxivar els fitxers amb dades de caràcter personal a la carpeta indicada pel Responsable de Seguretat, a fi de facilitar l'aplicació de les mesures de seguretat que corresponguin.

e) Els empleats tenen terminantment prohibit l'enviament d'informació de caràcter personal de nivell alt, llevat d'autorització expressa del Responsable de Seguretat. En tot cas, l'enviament d'aquesta documentació només es pot fer amb l'adopció prèvia dels mecanismes necessaris per evitar que la informació no sigui intel·ligible ni manipulada per tercers.

3.4. **OBLIGACIONS RESPECTE ALS FITXERS NO AUTOMATITZATS**

a) Mantenir degudament custodiades les claus d'accés a l'organització/comunitat educativa, despatxos i armaris, arxivadors o elements que continguin fitxers no automatitzats, amb dades de caràcter personal. S'haurà de comunicar al Responsable de Seguretat qualsevol fet que pugui haver compromès aquesta custòdia.

b) Tancar els despatxos al final de la jornada laboral o quan se n'absenti temporalment, per evitar accessos no autoritzats.

c) Establir procediments de copiat o reproducció de documents per tal que puguin fer aquestes tasques les persones habilitades pel Responsable de Seguretat.

4.- **INCOMPLIMENT**

4.1. **COMUNICACIÓ**

En cas d'infracció de les presents normes COL·LEGI MARE DE DÉU DEL CARME comunicarà a l'empleat, tan aviat tingui coneixement dels fets i li sigui possible, la infracció comesa i les seves conseqüències.

4.2. **CONSEQÜÈNCIES**

L'organització/comunitat educativa disposa de diferents mitjans davant de l'incompliment de les obligacions contingudes en aquest document:

a) Podrà incoar un expedient disciplinari a l'empleat amb les corresponents sancions previstes pel Conveni Col·lectiu o legislació laboral.

b) Si com a conseqüència de l'actuació de l'empleat, l'organització/comunitat educativa fos objecte de sanció o responsabilitat, o hagi d'abonar alguna indemnització per danys, de qualsevol ordre, podrà repetir contra l'empleat l'import de la quantitat que hagués hagut d'abonar més, si escau, les despeses que això li hagi ocasionat.

5.- **VIGILÀNCIA I CONTROL PER PART DE COL·LEGI MARE DE DÉU DEL CARME.**

Les eines informàtiques són posades a disposició dels empleats per part de COL·LEGI MARE DE DÉU DEL CARME, amb fins exclusivament professionals, per la qual cosa aquestes han de ser utilitzades única i exclusivament amb aquesta finalitat, amb les excepcions previstes en aquest Protocol (si s'acorda possible ús personal i privat).

Per això, COL·LEGI MARE DE DÉU DEL CARME es reserva el dret de comprovar, quan ho consideri convenient, si la utilització que es fa d'aquests recursos s'ajusta a la finalitat que li és pròpia, i al que preveu aquest Protocol.

Tipus de control:

- ***Procediment de control roman*nte** i sense avís previ a l'empleat a fi de comprovar, a través dels programes necessaris i imprescindibles, la utilització que s'estigui fent de les eines informàtiques posades a disposició dels empleats.
- **Procediment de control mitjançant l'accés als equips informàtics**. Aquest es pot dur a terme quan hi hagi indicis d'incompliments de les mesures establertes en aquest protocol, en funció de les circumstàncies concurrents, i d'acord amb el procediment següent:
    - S'ha de fer sempre en presència de l'empleat a qui estigui assignat l'equip sotmès a revisió i dins de la jornada de treball. Si l'empleat s'hi nega, s'ha de deixar constància en acta aixecada a aquest efecte.
    - La revisió es farà a presència d'almenys dos representants legals dels empleats, sempre que l'usuari l'equip del qual

s'examinarà ho sol·liciti, llevat que aquells es neguin a ser-hi presents.

- COL·LEGI MARE DE DÉU DEL CARME designarà un representant que podrà comptar amb el suport i l'assessorament d'una o diverses persones amb coneixements informàtics.

- L'empleat afectat té obligació de facilitar l'accés al seu equip informàtic, per a això proporcionarà les claus necessàries. Si l'empleat s'hi nega, s'ha de fer constar aquesta negativa i, si s'escau, es poden adoptar les mesures tècnico-informàtiques necessàries per a aquest accés a l'equip i als diferents programes.
- Els arxius i la resta de documents que es considerin d'interès a efectes de provar l'incompliment, s'imprimiran en paper i se signaran per tots els presents, quedant sota la custòdia de la Direcció de COL·LEGI MARE DE DÉU DEL CARME. Si algun dels presents es negués a la signatura es deixarà constància a lacta. Com a alternativa a la impressió, es podrà fer dues còpies de seguretat, i en quedarà una dipositada en lloc que en garanteixi la custòdia i la intangibilitat. L'altra podrà ser objecte de revisió per part de COL·LEGI MARE DE DÉU DEL CARME.

- S'aixecarà acta de tot el que s'esdevingui en què s'indicarà:
  a) Nom, cognoms i DNI dels assistents i qualitat en què són presents.
  b) Motiu de la revisió i actuacions que es duran a terme.
  c) Breu descripció del resultat de les actuacions.
  d) Possibles incidències

<u>Regles per a la revisió del correu electrònic</u>:

COL·LEGI MARE DE DÉU DEL CARME podrà establir els mecanismes necessaris perquè el sistema informàtic pugui detectar el nombre de correus remesos i adreces. Pel que fa al contingut, es distingirà entre correus personals i no personals.

Pel que fa als correus no personals, COL·LEGI MARE DE DÉU DEL CARME tindrà total llibertat de revisió.

Pel que fa als correus personals només podran ser revisats en els casos següents:

- Quan hi hagi indicis raonables que s'està utilitzant per cometre infraccions administratives o penals.
- Quan es pugui raonablement presumir l'existència d'assetjament i altres tipus d'actuació delictiva, mitjançant

correu electrònic, a subordinats, clients, proveïdors, o persones vinculades a COL·LEGI MARE DE DÉU DEL CARME.

La revisió es durà a terme en els termes indicats per accedir als equips informàtics.

ANNEX 2: PROPOSTA A SEGUIR EN EL SISTEMA D'INFORMACIÓ ALS EMPLEATS

S'aconsella en primer lloc comunicar les normes esmentades al Comitè d'Organització/comunitat educativa.

Un cop comunicada i informats a aquests representants, es donarà a conèixer tots els empleats a través del medi que es consideri més convenient:

a) Realitzar enviament d'una circular i comunicar que aquest Reglament i Política d'Ús de TIC's i Protecció de Dades Personals estan disponibles a la Intranet de COL·LEGI MARE DE DÉU DEL CARME.

b) Realitzar xerrades de formació on s'expliqui aquestes normes d'ús, comunicant que estan a la vostra disposició a la Intranet de L'ORGANITZACIÓ/COMUNITAT EDUCATIVA per a la vostra consulta.