

MANUAL DE BONES PRÀCTIQUES

FUNDACIÓ SANT GREGORI – ESCOLA GALÍ BELLESGUARD

NIF - G-58004185

Carrer Carles Riba nº 11-15

08035 Barcelona

Delegat de Protecció de Dades: dpd@galibellesguard.cat

Per tal de garantir la confidencialitat i seguretat de les dades personals, de conformitat amb el Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (en endavant, referit com a RGPD), l'organització FUNDACIÓ SANT GREGORI (referida en endavant com l'organització) ha establert les següents instruccions de seguretat, que haurà de complir tant el personal contractat com el personal col·laborador.

MESURES GENERALS

1. Les dades de caràcter personal a què tingui accés el personal contractat o col·laborador només seran utilitzades amb la finalitat de desenvolupar les funcions pròpies del lloc de treball, garantint el compromís de confidencialitat i l'ètica professional.
2. El tractament de les dades només es podrà fer amb els recursos, suports, dispositius, equips i entorns informàtics autoritzats per l'organització. Resta totalment prohibit fer servir altres mitjans o recursos diferents dels indicats. De la mateixa manera, no poden fer-se servir mitjans de transmissió de la informació diferents dels proveïts pels serveis informàtics de l'organització.
3. Resta prohibit de manera general treballar fora dels entorns informàtics habilitats per l'organització. En particular, resta prohibit desar informació en unitats de memòria locals i fer servir dispositius de memòria (per exemple, USBs) per al tractament de les dades sense el coneixement i l'autorització expressa i prèvia de l'organització o dels seus responsables.

4. Resta prohibida la descàrrega de documents que continguin dades de caràcter personal en un equip informàtic o dispositiu mòbil sense el coneixement i l'autorització expressa i prèvia de l'organització. En cas que sigui necessària fer la descàrrega, un cop finalitzada la necessitat que l'hagi motivat, caldrà eliminar les dades de caràcter personal del dispositiu o equip.
5. Resta totalment prohibit fer servir telèfons mòbils personals o altres dispositius personals per a fer fotos o gravacions d'àudio o vídeo a les àrees de treball de l'organització o per a transmetre dades personals relatives al lloc de treball sense el coneixement i l'autorització expressa i prèvia de l'organització.

ACCÉS INFORMÀTIC I CLAUS D'ACCÉS

6. Cada usuari amb accés informàtic autoritzat tindrà cura que les dades que es visualitzin per pantalla o que s'imprimeixin no puguin ser accedides per persones no autoritzades.
7. Quan un membre del personal finalitzi la seva jornada laboral o abandoni el seu lloc de treball durant un període de temps determinat, tancarà les aplicacions amb què ha estat treballant, finalitzarà la seva sessió com a usuari i apagarà l'ordinador.
8. El personal laboral o col·laborador és responsable de la vigilància i confidencialitat de les claus d'accés als entorns informàtics de tractament de dades proveïts per l'organització. En cas que aquestes claus siguin conegudes o difoses entre persones no autoritzades, caldrà comunicar-ho al DPD i tractar-ho com a incidència de seguretat.
9. Resta totalment prohibit que un membre del personal accedeixi a una història clínica o informació de salut d'una persona, si això no forma part de les funcions del seu lloc de treball. L'organització realitzarà accions periòdiques de revisió d'accessos informàtics a les històries clíniques, a fi de detectar possibles accessos indeguts o injustificats, els quals seran sancionats.

10. Cada membre del personal haurà de procedir al canvi de la seva contrasenya quan el sistema ho requereixi. De la mateixa manera, es mantindrà una mesura de bloqueig de l'accés després d'un període d'inactivitat. El sistema es configurarà de manera que el desbloqueig requereixi la clau d'accés. Aquestes mateixes mesures s'han d'implementar especialment en els equips de personal que treballi remotament o faci teletreball, sempre que s'hagi autoritzat prèviament el tractament remot de les dades per part de l'organització.

ÚS D'INTERNET I CORREU ELECTRÒNIC

11. L'ús d'internet es limitarà a qüestions directament relacionades amb l'activitat de l'entitat i amb el lloc de treball de l'usuari.
12. Resta prohibit introduir, descarregar d'Internet, reproduir, utilitzar o distribuir programes informàtics no autoritzats per part de l'entitat.
13. Sempre que s'hagin d'enviar dades de salut per correu electrònic, s'aplicaran mesures de xifratge o d'encriptació, per tal que la informació només sigui accessible a través d'una contrasenya. A aquest efecte, es tindran en compte les instruccions o protocols aprovats per l'àrea informàtica de l'entitat.

DOCUMENTACIÓ EN PAPER

14. Sempre que no es faci servir, es mantindrà la documentació en paper que contingui dades de caràcter personal correctament desada i ordenada en calaixos o armaris tancats amb clau.
15. Sempre que s'hagi de destruir documentació en suport paper que contingui dades de caràcter personal, caldrà fer-ho de forma segura i confidencial, garantint l'eliminació de les dades. D'aquesta manera, és obligatori que el paper es destrueixi a través d'una màquina trituradora o d'un servei extern especialitzat. Aquesta mesura és necessària per a evitar el risc d'accés a les dades per part de persones no autoritzades.

16. Resta totalment prohibit treure de les àrees de treball històries clíniques o documentació que contingui dades de salut sense l'autorització expressa i prèvia de l'organització.

ÚS DE SUPORTS I DISPOSITIUS DE L'EMPRESA

17. L'ús de suports i dispositius de l'empresa es limitarà a qüestions directament relacionades amb l'activitat de l'entitat i amb el lloc de treball de l'usuari.
18. Cal que els equips, suports i dispositius informàtics o electrònics que continguin dades personals estiguin clarament identificats; que es conegui de manera inequívoca qui són l'usuari o els usuaris que hi tenen accés.
19. Resta totalment prohibit que qualsevol suport o document en paper, dispositiu electrònic, suport o equip informàtic que contingui dades de caràcter personal surti de les àrees de treball sense el coneixement, autorització expressa i control de l'organització.
20. Quan es deixi d'utilitzar un suport informàtic o dispositiu electrònic que contenia dades de caràcter personal, cal que se n'esborri tota la informació i que s'adoptin mesures destinades a prevenir l'accés o la recuperació de les dades personals.

NOTIFICACIONS AL DPD

21. Sempre que es detecti qualsevol incidència, anomalia o violació en el tractament de les dades o en la seva seguretat, caldrà notificar-ho immediatament al DPD a dpd@galibellesguard.cat, posant en còpia l'equip directiu. Així, per exemple, s'ha de comunicar al DPD (amb còpia a Direcció) qualsevol situació de pèrdua o d'error en el tractament de les dades o qualsevol situació de risc.
22. Sempre que es plantegi fer un tractament de dades amb una nova tecnologia, caldrà posar-ho en coneixement del DPD, per tal que n'analitzi els riscos.

23. Sempre que es detecti una situació de risc en el tractament de les dades, caldrà posar-ho en coneixement del DPD.

24. Per a qualsevol dubte sobre la interpretació d'aquestes instruccions o per a l'autorització de determinades operacions de tractament de dades que estan generalment prohibides, el personal de l'organització pot adreçar-se al DPD o als responsables designats.

RÈGIM SANCIONADOR

La incorporació a la dinàmica de l'organització dels principis rectors de la Protecció de Dades de Caràcter Personal adquireix una gran importància en la mesura que el seu incompliment pot comportar greus responsabilitats tant per a l'organització com per al personal que tracta o accedeix a les dades de caràcter personal; a banda de sancions administratives destinades a l'organització, l'incompliment de les obligacions sobre protecció de dades pot derivar en responsabilitats personals de tipus civil, laboral i fins i tot penal. De forma particular, l'incompliment de les instruccions contingudes en aquest manual pot comportar la imposició de sancions per part de l'organització, de conformitat amb el règim laboral sancionador previst a l'Estatut dels Treballadors i al Conveni Col·lectiu vigent i aplicable.

Nom i DNI del Treballador/Col·laborador:

Data i signatura