PROTOCOL D'ÚS DE LA TECNOLOGIES DE LA INFORMACIÓ I LA COMUNICACIÓ (TIC)

ESCOLA JESÚS, MARIA I JOSEP

cipdi
COMPLIANCE

ÍNDEX

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

1.- OBJECTE

El present protocol regula l'ús de les Tecnologies de la Informació i la Comunicació (TIC) a l'escola, amb la finalitat de garantir els drets de tots els membres de la comunitat educativa quan es comuniquin mitjançant suports amb tecnologies digitals.

2.- ÀMBIT D'APLICACIÓ

2.1.- ÀMBIT OBJECTIU

Cal aplicar el present protocol a totes les activitats organitzades per l'escola o en les que hi participi.

També s'ha d'aplicar a les activitats que, tot i que no siguin organitzades per l'escola o hi participi activament, es produeixi relació entre els membres de la comunitat educativa fent servir suports digitals.

2.2.- ÀMBIT SUBJECTIU.

Tothom que es relacioni amb l'escola mitjançant les TIC està obligada a complir els requisits establerts en aquest protocol.

3.- DEFINICIONS

• **Accessos autoritzats**: Autoritzacions o permisos atorgats a un usuari per què pugui fer servir diversos recursos.

• **Administrador del sistema:** Usuari privilegiat del sistema informàtic que li permet canviar configuracions. Té la responsabilitat d'executar, mantenir, operar i assegurar el funcionament correcte d'un sistema informàtic i/o xarxa.

• **Autenticació**: Procediment de comprovació de la identitat d'un usuari. Garanteix que l'usuari que accedeix a un sistema d'ordinador és qui diu ser. En general, els sistemes d'autenticació estan basats en una clau, codi o contrasenya privada i secreta posada pel propi usuari.

• **Autenticador:** Codi d'accés, contrasenya.

• **Bloc:** Pàgina *web*, generalment de caràcter personal, amb una estructura cronològica que s'actualitza regularment i que presenta informació o opinions sobre temes diversos

• **Contrasenya**: Informació de caràcter confidencial, freqüentment constituïda per una cadena de caràcters, que es pot fer servir per a autenticar un usuari.

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

• **Còpia de suport**: Còpia de les dades d'un fitxer automatitzat a un suport que permeti la recuperació. Es pot desar al mateix lloc en el que s'ha fet la còpia.

• **Còpia de recuperació**: Còpia de les dades d'un fitxer automatitzat a un suport que permeti la recuperació. La còpia de recuperació s'ha de desar fora dels locals en els que estigui l'ordinador origen de la còpia.

• **Directoris de correu**: Conjunt d'adreces electròniques, estructurat per fer recerques. És un concepte similar al de "guia telefònica", aplicat a les adreces electròniques.

• **Domini o Nom de Domini**: És un nom registrat que identifica el lloc de la xarxa d'una organització accessible pels usuaris d'Internet. Per exemple, <cipdi.com> és el nom de domini del Centre Integral de Protecció de la Informació.

• **Driver**: Es un controlador de dispositiu, anomenat normalment controlador (en anglès, *device driver*) és un programa informàtic que permet al sistema operatiu interactuar amb un perifèric. El programa interactua amb un dispositiu extern a l'aparell que conté el sistema operatiu. El "*driver*" conté informació especifica sobre el dispositiu i fa de mitjancer entre el dispositiu i el sistema operatiu.

• **Firewall**: Aplicació de seguretat que regula i controla l'accés als sistemes connectats a Internet.

• **HTML (HyperText Markup Language)**: Llenguatge de marcat d'Hipertext. És el llenguatge estàndard per descriure el contingut i l'aparença de les pàgines en Internet. Els navegadors interpreten aquest llenguatge per presentar la informació a l'usuari.

• **HTTP (HiperText Transfer Protocol)**: Protocol de Transmissió Hipertext. Protocol de comunicacions utilitzat pels programes clients i servidors de WWW per comunicar-se entre si.

• **Identificador:** Símbol, caràcter o grup de caràcters, usat per a designar un element individual de les dades d'un programa**.**

• **Internet**: Xarxa digital de transmissió basada en el protocol TCP/IP que interconnecta entre si xarxes de menor mida, permetent la comunicació entre qualsevol parell d'ordinadors connectats a aquestes xarxes subsidiàries.

• **Núvol:** model que permet, de forma pràctica i des de qualsevol ubicació, l'accés sota demanda a una sèrie de recursos informàtics configurables compartits (xarxes, servidors, sistemes d'emmagatzematge, aplicacions i serveis), que poden ser ràpidament dotats i posats en funcionament amb un mínim esforç de gestió i interacció amb el proveïdor de serveis ".

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

• **Núvol públic:** És aquell tipus de cloud (núvol) en el qual la infraestructura i els recursos lògics estan sota el control del proveïdor de serveis que l'allotja, opera i gestiona, estant disponible per al públic en general.

• **Núvol privat:** D'ús exclusiu per a una organització, es crea generalment amb recursos propis de l'empresa.

• **Núvol comunitari:** Un cloud comunitari es dóna quan dues o més organitzacions integren una comunitat que comparteix interessos i comparteixen els beneficis d'una infraestructura cloud comuna, que es gestiona per una d'elles o per una tercera part en nom seu.

• **Núvol híbrid:** La infraestructura és el resultat de la combinació de diverses de les anteriors, incloent-hi els mitjans per a la connexió i la portabilitat de la informació entre les diferents estructures

• **IRC (*Internet Relay Chat***): Xerrada Interactiva a Internet. Protocol per a converses simultànies que permet comunicar-se entre si a diverses persones en temps real.

• **Recurs**: Qualsevol part que integra un sistema d'informació.

• **Servidor Web**: És el programa que, utilitzant el protocol de comunicacions HTTP, és capaç de rebre peticions d'informació d'un programa client (navegador), recuperar la informació sol·licitada i enviar-la al programa client per a que l'usuari la pugui veure.

• **Servidor Web segur**: Servidor Web que utilitza protocols de seguretat (SSL o SHTTP generalment) quan executa transaccions. Un protocol de seguretat utilitza tècniques de xifrat i autenticació com instrument per incrementar la confidencialitat i la fiabilitat de les transaccions.

• **SHTTP (Secure HTTPS**): Sistema encaminat a proporcionar transaccions segures dins de l'entorn World Wide Web.

• **Sistema d'informació**: Conjunt de fitxers automatitzats, programes, suports i equips que es fan servir per a enregistrar i tractar dades.

• **Suport**: Objecte físic susceptible de ser tractat en un sistema d'informació i sobre el qual es poden gravar o recuperar dades. El suport no forma part de la informació. Així, les fotografies són suports que contenen informació sobre les persones. L'afectat té dret a la informació que contenen els suports i, de vegades, a la titularitat dels suports.

• **Spam**: Tramesa massiva de missatges publicitaris que el destinatari no ha demanat expressament, fent servir el correu electrònic. Els qui es dediquen a aquesta activitat reben el nom de "spammers".

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

• **SSL (Secure Sockets Layer**): El protocol de seguretat més usat en Internet. Fa servir criptografia asimètrica per generar una clau de sessió amb què es xifren les comunicacions entre el client i el servidor. Proporciona també serveis d'autenticació del servidor i, opcionalment, del client.

• **Transferència de dades**: el transport de dades entre sistemes informàtics per qualsevol mitjà de transmissió, així com el transport de suports de dades per correu o per qualsevol altre mitjà convencional.

• **Usuari**: Subjecte o procés autoritzat per accedir a dades o recursos. A efectes de la normativa sobre telecomunicacions, la persona que utilitza un servei públic de telecomunicacions amb finalitats privades o comercials, encara que no sigui ell directament qui hagi contractat aquest servei.

• **Xarxa pública de telecomunicacions**: Els sistemes de transmissió i, quan sigui procedent, els equips de commutació i altres recursos que permeten la transmissió de senyals entre punts d'acabament definits per cable, per mitjans radioelèctrics, per mitjans òptics o per mitjans electromagnètics que s'utilitzin, de manera total o parcial, per a la prestació de serveis públics de telecomunicacions.

• **Xifrat**: Transformació d'un missatge en un altre, utilitzant una clau per impedir que el missatge transformat pugui ser interpretat per aquells que no coneixen la clau.

4.- OBLIGACIONS GENERALS.

No es poden captar imatges, sons o dades de ningú sense el seu permís previ. Si la captació s'ha de fer a dins dels recintes de l'escola o durant una activitat escolar, cal tenir el permís previ de la direcció pedagògica.

Tota la comunitat educativa ha de mantenir el respecte degut a la resta de membres de la comunitat. Els membres de la comunitat educativa s'han d'abstenir de fer difusió de notícies falses, insults o ofenses de qualsevol tipus. Si s'ha comunicar qualsevol incidència, cal fer servir els canals oficials que l'escola posa a l'abast del personal i dels alumnes i les seves famílies.

S'ha d'identificar a tothom que tingui permís per a accedir al sistema d'informació de l'escola. A més a més de la identificació, cal establir un procediment d'autenticació. L'identificador i l'autenticador, en conjunt, s'anomena contrasenya.

L'autenticador ha de ser secret i intransferible. Si l'usuari detecta, o sospita que algú pot conèixer el seu codi autenticador, ho ha de posar en coneixement de la direcció, mitjançant una comunicació d'incidència.

La informació de la comunitat educativa que hi ha en el sistema de l'escola és

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

propietat de l'escola. S'han de fer còpies de seguretat de tota la informació que hi hagi al centre de tractament. Les còpies de seguretat han d'estar permanentment a disposició de la direcció.

El sistema d'informació de l'escola només es pot fer servir amb permís de la direcció.

Només es pot accedir a la xarxa interna de l'escola amb el codi identificador i el primer codi autenticador assignat per la direcció.

S'ha de bloquejar l'accés al sistema quan s'acabi de treballar en xarxa, o durant períodes d'inactivitat superior a cinc minuts.

La primera vegada que algú es connecti a la xarxa, ha de trobar un missatge quin contingut s'adjunta com a annex 1, que ha de ser acceptat expressament abans de procedir a la validació.

A la xarxa han d'haver-hi diferents tipus de carpetes:

a. **Carpetes personals:** són les que contenen informació de l'usuari. Només poden accedir-hi les persones que consenti prèviament el propi usuari.
b. **Carpetes compartides**: Carpetes a les que poden accedir-hi persones amb els mateixos privilegis. Per exemple: tots els coordinadors o la carpeta de l'equip directiu.
c. **Carpetes públiques:** Carpetes d'accés lliure als usuaris de la xarxa.

Cal respectar aquesta distribució de carpetes per evitar que persones sense permís accedeixin a informació classificada.

No està permès:

1. Compartir o facilitar la clau d'accés (contrasenya) a una altra persona física o jurídica, inclòs el personal del col·legi, ni que tingui més categoria jeràrquica. En cas d'incompliment d'aquesta prohibició, l'usuari es fa responsable dels actes que faci la persona física o jurídica que hagi simulat ser el titular de la contrasenya
2. Intentar distorsionar o falsejar els registres LOG del sistema.
3. Intentar desxifrar les claus, sistemes, o algoritmes de xifrat i qualsevol altre element de seguretat que intervingui en els processos telemàtics de l'escola
4. Destruir, alterar, inutilitzar o, de qualsevol altra forma, fer malbé les dades, programes, o documents electrònics de l'escola.
5. Obstaculitzar voluntàriament l'accés d'altres usuaris a la xarxa mitjançant el consum massiu dels recursos informàtics i telemàtics, així com fer accions que facin malbé, interrompin, o generin errors en els sistemes.

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

6. Enviar missatges de correu electrònic de forma massiva o amb finalitats comercials, o publicitàries sense el consentiment del destinatari (Spam).
7. Intentar llegir, esborrar, copiar, o modificar els missatges de correu electrònic o arxius d'altres usuaris.
8. Fer servir el sistema per intentar accedir a àrees restringides dels sistemes informàtics de l'escola.
9. Intentar augmentar el nivell de privilegis d'un usuari del sistema, sense el permís exprés de la direcció.
10. Introduir voluntàriament programes, virus, macros, applets, controls ActiveX o qualsevol altre dispositiu lògic o seqüència de caràcters que causin, o siguin susceptibles de causar, qualsevol tipus d'alteració als sistemes informàtics de l'escola sense el permís de la direcció.
11. Introduir, descarregar d'Internet, reproduir, utilitzar o distribuir programes informàtics o arxius que no estiguin autoritzats expressament per la direcció de l'escola.
12. Instal·lar còpies il·legals de qualsevol programa, incloses les dels estandarditzats.
13. Esborrar qualsevol dels programes instal·lats legalment.
14. Fer servir els recursos telemàtics de l'escola per fer activitats que no es trobin directament relacionades amb el lloc de treball de l'usuari.
15. Introduir, consultar o descarregar continguts obscens, immorals o ofensius i, en general, mancats d'utilitat per assolir els objectius de l'escola.
16. Enviar o reexpedir missatges en cadena o de tipus piramidal sense permís de la direcció.
17. Accedir i/o fer servir informació sobre persones físiques o jurídiques identificades o identificables a la xarxa sense el permís de la direcció.
18. Fer servir suports de qualsevol tipus, núvols, correus electrònics, xarxes socials, xats, pàgines de noticies, blocs i programes de descàrrega, sense permís de la direcció.

S'ha de bloquejar l'accés dels usuaris quan s'acabi la relació entre l'usuari i el centre de tractament, o quan es detecti que l'usuari ha fet alguna de les activitats que no estan permeses.

Per motius de seguretat, la circulació d'informació per la xarxa pot ser monitorada. L'escola disposa de firewall i filtres de continguts que monitoren el trànsit de dades.

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

5.- ELS ALUMNES.

5.1.- ÚS DE SUPORTS

Els alumnes només poden fer servir els suports que estiguin autoritzats expressament en aquest protocol o, particularment, pels professors quan estan a la seva classe.

S'ha de permetre que els alumnes facin servir suports de l'escola quan es limiti a fer activitats docents i dirigides per un professor. Quan els alumnes acabin de fer servir els suports, els han de deixar en les mateixes condicions que se'ls van trobar.

Extraordinàriament, si a algun alumne li cal fer servir un suport propi, ha de demanar permís al professor, justificant la finalitat. Si justifica l'ús extraordinari i no perjudica el normal funcionament de la classe, el professor podrà autoritzar-ne l'ús.

Els suports que no siguin titularitat de l'escola han de romandre tancats i desats durant l'horari lectiu i no lectiu. És possible que els professors autoritzin als alumnes que facin servir suports propis. En aquest cas:

- Només es podran fer servir quan l'ús estigui prèviament autoritzat per un professor degudament habilitat (professor, tutor, coordinador o cap d'estudis de l'alumne).

- Els alumnes son els únics responsables dels seus aparells, de l'ús i del manteniment, així com de la cura i control de la possessió.

- Els alumnes han de portar sempre a l'escola els suports personals que hagin de fer servir durant l'horari lectiu, carregat elèctricament i amb la configuració de programari indicada pel professor que n'autoritzi l'ús.

- Els suports han d'estar identificats amb un adhesiu on hi consti el nom del propietari/a i el número de sèrie.

- Els suports s'han d'iniciar quan ho digui el professor i han de romandre inactius si el professor ho demana.

- Quan s'hagi acabat l'activitat, cal tancar i es desar-lo als espais que digui el professor.

- No es poden fer servir suports d'una altra persona, però, si el docent ho creu oportú, sota la seva responsabilitat, es poden compartir sempre amb que estigui present el propietari.

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

- No està permès fer servir els ordinadors al pati, als passadissos, al menjador i en els espais d'esbarjo, sense una autorització expressa (per escrit) d'un professor habilitat.

- Només es poden fer servir auriculars i “webcams” quan ho permeti un professor habilitat.

- Ningú no pot accedir als continguts d’un suport personal dels alumnes sense el seu permís. En cas que un professor sospiti que en el suport d’un alumne hi ha proves d’alguna infracció (civil i/o penal) o que vulnera alguna de les normes establertes en el reglament del centre, pot intervenir l’ordinador.

- La intervenció de l’ordinador s’ha de fer seguint el següent procediment:

  1. Requeriment: El professor ha de requerir (ordenar) l’alumne que tanqui l’aparell completament.
  2. Remissió: Si ‘alumne obeeix i tanca l’ordinador, se l’ha de enviar a la direcció a fi de que el director disposi el que calgui després que el professor notifiqui la incidència i la valoració del risc.
  3. Obertura i accés als continguts: El director pot demanar a l’alumne que obri l’aparell i que li doni accés als continguts controvertits a fi de fer les comprovacions que calguin.
  4. Intervenció del representant del menor: En cas de que l’alumne es negui a obrir l’accés als continguts requerits, el director podrà requerir la compareixença a l’escola del representant legal de l’alumne a fi de procedir a la diligència.
  5. Si el representant del menor no compareix, o es nega a complir la diligència, se l’obligarà a rebre l’aparell, tancat, a signar el rebut en el que consti la incidència i, simultàniament, el director ordenarà obrir un expedient disciplinari contra l’alumne pel motiu que hagi notificat el professor a la seva incidència. (Annex 2)

5.2.- ÚS DEL SISTEMA DIGITAL DE L’ESCOLA

Els alumnes han de tenir accés autoritzat a la xarxa interna de l’escola per fer les feines encomanades pels professors. En alguns casos, també cal que tinguin accés a la xarxa externa (internet). L’accés a la xarxa s’ha de limitar a l’activitat docent i s’ha de restringir tècnicament impedient l’accés als llocs o als continguts que l’escola consideri que no són apropiats.

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

S'ha de sancionar el fet de fer servir els sistemes de tractament i/o la informació de l'escola sense permís.

Els representants legals dels alumnes s'han de fer responsables de l'ús que facin de la xarxa de l'escola els seus representats. Cal que signin el document d'assumpció de responsabilitat (annex 3).

5.2.1.- El correu electrònic dels alumnes.

Per fer servir el correu electrònic, cal tenir present:

- Alumnes més grans de 14 anys. Poden fer servir el correu electrònic sense el permís del seu representant legal. No obstant això, cal que els representants legals estiguin informats de la creació i us del correu.

- Alumnes més petits de 14 anys. Cal el consentiment específic d'un del representant legal.

El correu electrònic corporatiu només es pot fer servir amb finalitats pròpies de l'escola. Es pot fer servir per donar-se d'alta de servei telemàtics de l'escola.

Convé que no es faci servir aquest correu per a finalitats alienes a la docència.

No es poden enviar correus massius fent servir comptes corporatius.

Quan es creïn comptes nous convé que es faci servir un pseudònim.

5.3.- ÚS DE SISTEMES ALIENS A L'ESCOLA

Les NOFC i les normes de convivència s'apliquen a totes les activitats organitzades per l'escola i a totes en les que hi participi, tant si es fan presencials o per via telemàtica. La captació, l'ús i la difusió de dades, informació i imatges de persones físiques sense permís dels interessats s'ha de sancionar.

En les activitats escolars s'han de fer servir els sistemes de l'escola. Només es poden fer servir suports particulars amb permís exprés de la direcció.

No està permès crear perfils que simulin la identitat de l'escola o la impliquin de qualsevol manera sense el permís de la direcció del centre.

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

6.- ELS REPRESENTANTS LEGALS DELS ALUMNES

Els representants legals:

- Han de signar ell document de compromís d'ús responsable de les eines TIC. El formulari consta adjunt com a Annex 3,

- En l'ús responsable de la tecnologia han de ser un exemple pels seus fills.

- Han donar suport i col·laborar en les decisions de l'escola i, especialment, quan s'hagi de corregir la conducta dels alumnes en el cas de les sancions per ús indegut o no autoritzat de la tecnologia.

- Han de complir i fer complir als seus fills les normes de seguretat que l'escola recomani.

6.1.- ÚS DE SUPORTS

Els representants legals dels alumnes estan obligats a controlar els suports que proporcionin als seus fills i els drets de connexió a internet (comptes de telèfon). Si no poden garantir el control dels suports que els alumnes porten a l'escola, han d'avisar el tutor a fi de que l'escola prengui les mesures de seguretat preventives adequades a cada situació.

Quan facin servir suports dins del recinte escolar , ho han de fer de manera que no perjudiquin el dret d'altres persones, especialment, en relació a la captació, reproducció i conservació de dades.

6.2.- ÚS DEL SISTEMA DE L'ESCOLA

Els identificadors i els autenticadors que l'escola faciliti als representants legals per accedir al sistema de l'escola són personals i intransferibles. En cas que es detecti un accés il·legítim cal que es comuniqui al tutor.

Els representants legals es poden connectar al sistema de l'escola si disposen de l'autorització de la direcció. Si es connecten, s'han d'abstenir de fer actuacions contraries a les lleis i al caràcter propi de l'escola.

Com a usuari o usuària, s'ha de fer servir el sistema de forma diligent i correcta i s'ha de comprometre a no fer-lo servir per fer activitats contràries a la llei, a la moral, als bons costums acceptats, a no fer res que, de qualsevol manera, pugui

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

danyar, inutilitzar, sobrecarregar, deteriorar o impedir el normal funcionament del sistema.

Els usuaris son els únics responsables de les conseqüències que es derivin de la vulneració d'aquestes obligacions.

L'escola no es fa responsable dels danys i perjudicis que es puguin derivar d'interferències o avaries telefòniques, desconnexions en el sistema electrònic, presència de virus informàtics, programes maliciosos o qualsevol altre factor aliè al seu control.

Fent servir els sistemes escolars, els usuaris exoneren de responsabilitat a l'escola per:

a. L'absència de disponibilitat i continuïtat d'accés al sistema.

b. La interrupció, suspensió o cancel·lació de l'accés.

c. La informació transmesa pels usuaris a través del canal subministrat pel servei d'accés.

d. Els danys i perjudicis de tota naturalesa per ús indegut del sistema.

e. Accessos no autoritzats a llocs protegits d'Internet, fent servir qualsevol tècnica de "hacking", "cracking", etc.

f. La disponibilitat tècnica, qualitat, exactitud o veracitat dels continguts i serveis disponibles de tercers als quals es pot accedir com a usuari o usuària des del sistema de l'escola.

7.- EL PERSONAL DOCENT I NO DOCENT DE L'ESCOLA

7.1.- ÚS DE SUPORTS

La informació sempre ha d'estar custodiada per una persona degudament habilitada per la direcció i, en el seu cas, ha de romandre tancada de manera que només hi puguin accedir les persones autoritzades pel responsable del tractament.

Els suports que continguin dades de caràcter personal han de ser desats aplicant criteris de finalitat. No es poden desar plegats suports que continguin dades que puguin ser consultades per persones que no tinguin el permís preceptiu.

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

7.1.1.- Còpia o reproducció.

Només es poden fer còpies dels documents que continguin dades especialment protegides amb el permís exprés de la direcció. Quan ja no sigui útil, la còpia s'ha de destruir.

S'ha de fer un inventari de tots els suports que siguin titularitat de l'escola. Cal dissenyar un tipus d'etiqueta que contingui una advertència clara sobre el contingut dels suports que continguin informació amb una prohibició d'accés al personal que no tingui permís o no estigui autoritzat expressament per la direcció. S'ha de deixar constància del contingut de cada suport en un llistat l'accés al qual ha de ser autoritzat expressament per la direcció.

Els discos durs dels PC que contenen dades han d'estar identificats i degudament custodiats. Qui tingui accés, respon de la informació accedida. Si l'accés és lliure, respon qui tingui les claus d'accés.

Si el disc dur no té clau d'accés, el responsable del departament ha de respondre dels accessos que es produeixin. Si el suport (PC, portàtil, etc.) es troba en un lloc d'accés lliure, el responsable de seguretat respon del tractament que es faci de les dades tractades .

Cal desar els suports físics que no es facin servir en un lloc tancat amb clau.

7.1.2.- Emmagatzematge dels suports.

Si prèviament s'ha obtingut l'autorització expressa de la direcció, es pot emmagatzemar en el núvol qualsevol arxiu que contingui dades de l'escola. S'entén que l'autorització és expressa, si es pot reproduir en algun suport en qualsevol moment i en qualsevol lloc.

Els suports que continguin dades de l'escola s'han d'emmagatzemar en llocs als que no puguin accedir-hi persones sense permís.

Suports homologats per la direcció per allotjar dades:

- Disc dur dels PC autoritzats com a suport permanent
- Suports especials homologats expressament per la direcció per fer còpies de seguretat.
- Llapis digitals "Pendrives" en els casos en què la direcció ho autoritzi per escrit.

Està prohibit allotjar dades en suports que no estiguin homologats.

El local on es desin els suports ha d'estar equipat amb mesures antiincendis.

7.1.3.- Control de sortida de suports amb dades.

Per treure un suport de l'escola, cal disposar de l'autorització expressa de la direcció. Aquesta autorització es pot atorgar des de qualsevol departament designat expressament pel director.

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

Cal gestionar un llibre registre, que pot ser un full Excel o similar, en el qual quedi constància dels requisits que cal complir per treure de l'escola suports amb dades.

Els documents, programacions, treballs, notes, apreciacions, incidències, llistes, encàrrecs, planificacions, i projectes en què intervinguin dades o informació del centre o de la classe, es podran treure de l'escola sempre que la persona que tregui la informació conegui i accepti les obligacions imposades al reglament intern de seguretat en matèria de tractament, gestió i seguretat de la informació i de les dades, i es comprometi a observar els seus preceptes en el lloc on hagi de tractar la informació que ha tret.

Quan es traslladi informació fora del centre, cal xifrar les dades de manera que es garanteixi que aquesta informació no pugui ser accedida o manipulada durant el transport. Tanmateix, s'han de xifrar les dades contingudes en els dispositius portàtils quan es trobin fora de les instal·lacions que estan sota el control de l'escola.

7.1.4.- Destrucció de suports.

Les dades només es poden destruir si ho permet el director.

Els suports que continguin informació sobre persones identificades o identificables s'han de destruir quan la informació hagi servit per a complir les finalitats per a les quals es va demanar.

Es considera que un suport està destruït quan sigui impossible recuperar la informació que contenia.

Cal formatar els suports informàtics o digitals que s'hagin de rebutjar, o es vulguin reutilitzar amb una altra informació diferent de la que hi havia.

7.2.- ÚS DEL SISTEMA DE L'ESCOLA

Només es podrà fer servir el sistema de l'escola per a activitats relacionades amb el lloc de treball. Quan es connectin al sistema de l'escola, el usuaris s'han d'abstenir de fer actes contraris a les lleis i al caràcter propi. Com a usuaris, s'ha de fer servir el sistema de l'escola de forma diligent i correcta i s'han de comprometre a no fer-lo servir per fer activitats contràries a la llei, a la moral, als bons costums acceptats i / o amb fins o efectes il·lícits, prohibits o lesius de drets i interessos de terceres persones, així com a no fer cap tipus d'ús que de qualsevol forma pugui danyar, inutilitzar, sobrecarregar, deteriorar o impedir el normal funcionament del sistema. L'usuari es l'únic responsable de les conseqüències que es derivin de la vulneració d'aquestes obligacions.

Els usuaris del sistema informàtic només han de tenir accés a la informació i als recursos que els calen per fer la feina encomanada per la direcció.

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

7.2.1.- La monitorització del sistema.

Només es pot accedir a les xarxes públiques com Internet, si ho permet fefaentment la direcció.

La direcció de l'escola té dret a "monitoritzar" i comprovar, de manera aleatòria, i sense avís previ, qualsevol sessió d'accés a Internet o a xarxes públiques iniciada per un usuari connectat al sistema de l'escola.

L'accés a pàgines web, grups de notícies, i altres d'altres fonts d'informació s'ha de limitar a les pàgines que continguin informació relacionada amb l'activitat de l'usuari dintre de l'escola.

7.2.2.- La gestió d'informació a través del correu electrònic.

Cap missatge de correu electrònic de l'escola es considera privat. Tots els missatges que entrin o surtin pel domini, o fent servir els mitjans de l'escola, es consideren correu de l'escola. Es considera correu electrònic, tant l'intern, entre terminals de la xarxa, com l'extern, dirigit, o procedent, altres xarxes públiques o privades, i, especialment, d'Internet.

La direcció de l'escola pot revisar, sense avís previ, els missatges de correu electrònic dels usuaris de la xarxa corporativa, els arxius LOG dels servidors, els programes instal·lats al servidor, o en els llocs de treball, i, en definitiva, qualsevol dels recursos que integren el sistema d'informació de l'escola sense necessitat d'avisar prèviament els usuaris, donat que abans d'adquirir els drets d'usuari, l'escola ha informat degudament i amb caràcter previ vers els sistemes de control d de l'ús .

Quan es vulguin enviar dades per correu electrònic, o per sistemes de transferència de base de dades, a través de xarxes públiques o xarxes que no estiguin protegides, cal encriptar la informació, de manera que només la pugui accedir el destinatari.

7.2.3.- Identificació i autenticació.

L'identificador té dues funcions: la primera, identificar l'usuari autoritzat; i la segona, definir la capacitat d'obrar de l'usuari dins del sistema.

Comprovats els límits a la capacitat d'obrar de l'usuari autoritzat, i, dotat d'un codi identificador, el responsable de seguretat ha de crear codis alfanumèrics, com a mínim, de vuit dígits, que s'associaran a l'identificador perquè el sistema pugui reconèixer a la persona que pretén accedir-hi.

L'autenticador equival a la signatura física; per tant, ha de ser personal, secret i intransferible. Només poden tenir accés al procediment per a assignar-lo, el responsable de seguretat i la direcció. Quan s'assigni un identificador i es comprovin els límits de la capacitat d'obrar dels usuaris amb permís d'accés, el responsable de sistemes de seguretat ha d'establir un procediment per construir

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

els codis alfanumèrics de vuit dígits perquè el sistema pugui reconèixer els usuaris que pretenguin accedir-hi.

Com a mínim, els autenticadors han de complir 3 dels requisits de complexitat:

Han de contenir:

1. lletra majúscula
2. lletra minúscula
3. un número
4. un símbol

Els usuaris han de conservar en secret els codis d'accés, perquè són els únics responsables de les conseqüències que puguin derivar de l'ús incorrecte, cessió voluntària, o involuntària, divulgació, o pèrdua del codi que configura la contrasenya.

Les operacions que es facin al sistema de l'escola han de quedar gravades en els arxius "log" dels servidors. L'ús de l'identificador i la clau assignats als usuaris implica l'acceptació dels registres generats en els arxius emmagatzemats en el sistema informàtic de l'escola com a document probatori de l'operació efectuada.

S'entén que els actes que es duguin a terme amb l'identificador i amb la clau assignats els ha fet el titular, tot i que hi hagi proves de que hagi estat utilitzat per una tercera persona.

7.3.- ÚS DE SISTEMES ALIENS A L'ESCOLA

S'entén sistema aliens a l'escola qualsevol suport, núvol, programa, xarxa o conjunt de dispositius que no estigui sota el control de l'escola.

L'ús de sistemes aliens a l'escola està prohibit amb l'excepció que hi hagi una autorització expressa per part de la direcció de l'escola i del DPD.

Qui pretengui fer servir un sistema aliè, cal que ho comuniqui a direcció. Per a què un sistema aliè sigui autoritzat, s'ha de valorar:

- La utilitat del programa. S'ha de veure si el programa és útil per l'escola i que no es pot fer servir cap dels sistemes homologats per l'escola.
- L'impacte per a la privacitat. Per valorar aquest aspecte cal:
    - Verificar si existeix alguna vulnerabilitat publicada del sistema.
    - Si el sistema està gestionat per una empresa ubicada a l'espai Schengen o, subsidiàriament, ubicada als EEUU però que garanteix el compliment del RGPD.
    - Si l'empresa que gestiona el sistema disposa d'una política de privacitat transparent.

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

- Verificar el tipus de dades que es fan servir.

L'usuari es l'únic responsable de les conseqüències que se'n puguin derivar de fer servir sistemes no autoritzats a dins del recinte escolar i de fer servir els sistemes homologats per fer actuacions que no estan permeses, o son prohibides.

8.- CIBERDELICTES

Són ciberdelictes els actes tipificats com a delictes al codi penal que es facin fent servir eines tecnològiques. Poden ser considerats ciberdelictes:

- Ciberassetjament o ciberbullying. L'assetjament, coaccions, amenaces, injúries i calumnies i/o danys morals i físics servint-se de mitjans tecnològics.
- Sexting. Fer-se fotografies, gravar-se en un vídeo o àudio, o deixar que ho facin altres en una situació compromesa o íntima quan estan implicats menors d'edat o quan es distribueix sense permís de l'interessat.
- Assetjament sexual o grooming
- Estafa
- Accés a comptes de correu, perfils de xarxes socials, etc. sense el permís del titular del compte o perfil.
- Spam. L'enviament indiscriminat de correus electrònics
- L'ús o introducció a un sistema de Malware o programes maliciosos que s'instal·len a l'equip i recullen dades de forma opaca
- Etiquetatge de fotos en xarxes socials per comprometre o perjudicar la víctima
- Suplantació de la identitat en xarxes socials
- Distribuir imatges o vídeos que atemptin contra la intimitat i la privacitat de les persones.
- Els insults i ofenses públiques.

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

- La imputació falsa d'uns fets

Qualsevol que conegui que algun membre de la comunitat educativa està implicat en un ciberdelicte, sigui com a autor o com a víctima, ha de fer servir el canal de denúncies de l'escola i posar-ho en coneixent de l'oficial de compliment.

9.- RÈGIM DISCIPLINARI

S'ha d'aplicar el protocol de reacció davant els incompliments.

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

ANNEXES

ANNEX 1.- MISSATGE D'INICI DE SESSIÓ

Us esteu connectant a la xarxa de l'escola Jesús, Maria i Josep. Per raons de seguretat us recordem que:

1.- L'usuari que us han facilitat és personal i intransferible. Si creieu que algú pot conèixer la vostra contrasenya, dirigiu-vos a .....

2.- Quan inicieu sessió, el sistema us demanarà que canvieu la contrasenya inicialment assignada. Introduïu la que vulgueu, però recordeu que ha de complir els següents requisits:

a) Ha de tenir un longitud mínima de 8 dígits.
b) Ha de combinar números i lletres.

3.- Cada tres mesos el sistema us demanarà que canvieu la contrasenya.

4.- Està prohibit desar qualsevol mitjà que us facilitem per identificar-vos, i autenticar-vos en ordinadors d'ús compartit.

5.- Deseu tots els documents a la vostra carpeta del servidor. És la única manera de garantir que podreu recuperar la informació en qualsevol moment.

6.- Tanqueu la vostra sessió quan no la feu servir.

7.- No està permès accedir, descarregar, i/o instal·lar, continguts o programes no autoritzats per la direcció. L'ús de les xarxes socials està expressament prohibit. Si necessiteu accedir a continguts no autoritzats, poseu-vos en contacte amb .....(la direcció de l'escola).

8.- Us recordem que per motius de seguretat les sessions informàtiques poden ser monitorades

9.- Si teniu qualsevol problema, o voleu augmentar els vostres privilegis assignats, contacteu amb .....

Acceptar i continuar

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

ANNEX 2.- DOCUMENT DE LLIURAMENT D'APARELLS INTERVINGUTS.

D. ..... amb DNI ....., pare, mare o tutor de l'alumne ..... pren possessió de..... (l'ordinador, tableta, mòbil,)..... nº de sèrie.....intervingut per la direcció el dia..... a les.....hores a .....(nom de l'alumne)

MANIFESTA:

1.- Que rep l'aparell apagat, tancat i en perfecte estat de conservació.

2.- Que a partir d'aquest moment, es fa responsable de l'ús i destí que se'n faci de l'aparell i de la informació que hi ha dins.

A.....el ..... de ..... de 20.....

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com

ANNEX 3.- ASSUMPCIÓ DE RESPONSABILITAT.

ASSUMPCIÓ DE RESPONSABILITAT DELS PARES VERS L'ÚS DELS APARELLS INFORMÀTICS, DE LES XARXES I DELS APARELLS PERSONALS ALS RECINTES DELS CENTRES DOCENTS.

En / Na ... ..., Pare / mare / tutor / .... / de ... ... (nom i cognoms de l'alumne menor d'edat) , amb el DNI N º ... ..., de manera voluntària i espontània,

DECLARO

I. - Conèixer les normes de conducta obligatòries exposades en el Reglament Intern de Seguretat del l'escola Jesús, Maria i Josep i, en especial, les que regulen l'ús dels aparells informàtics, digitals, documentals i de les xarxes.

II .- Que se m'ha notificat que als alumnes els està prohibit fer servir aparells que puguin gravar i/o connectar-se a internet, sense el permís exprés de la direcció de l'escola.

III .- Que se m'ha notificat que l'escola permet que els alumnes puguin dur aparells sempre que estiguin tancats i apagats, que no està permès fer servir les aplicacions de reproducció, navegació o gravació sense un permís exprés.

IV .- Que l'ús dels codis o claus d'accés a les xarxes privades de l'escola, als serveis digitals, i a les plataformes està sotmès a les condicions que consten en el Reglament Intern de Seguretat, el contingut del qual, dono per reproduït en la part necessària que, se m'informa, es troba a la meva disposició.

V. – Que en la representació que ostento de ... ... … ... .., demano que l'escola consenti i accepti que .....(nom de l'alumne) pugui portar suports de gravin, reprodueixin i/o naveguin i pugui fer servir les xarxes i els serveis digitals de l'escola durant el temps que romangui matriculat, en les condicions que consten al reglament del centre.

Reconec i faig meva la responsabilitat per les conseqüències que es puguin derivar de l'ús antireglamentari i de les infraccions que el meu fill pugui fer dels suports i dels sistemes dels que en sigui usuari dintre dels recintes de l'escola.

A fi de què consti a tots els efectes legals, el signo.

En ... ... a ... .. de ... ... de ... ...

Pare, mare o tutor

c/ Sant Agustí n. 1 1º 1ª – 08301 – Mataró –Barcelona – T. 934961845 – cipdi@cipdi.com