ESCOLA DE FORMACIÓ PROFESSIONAL
QUINTANES

PROTECCIÓ DE DADES ESCOLA EFA QUINTANES

ÍNDEX

1. Conceptes bàsics.

Què és el dret a la protecció de dades?
Dret a controlar l'ús que es fa de les nostres dades. El dret a la protecció de dades és un dret fonamental, que ve recollit a la nostra Constitució, Lleis Orgàniques i Europees, per exemple, la Carta Europea dels Drets fonamentals. És el dret que tenim els ciutadans a la nostra pròpia informació personal. Per tant, és el dret a controlar l'ús que es fa de les nostres dades i el que pretén és garantir a les persones un poder de disposició i control sobre les dades mitjançant l'exercici de determinats drets.

Què és una dada personal?
És tota informació d'una persona física que la identifica directament o la fa identificable (no hi entrarien les persones jurídiques):
Dades didentificació directa: nom i cognoms, DNI, imatge, etc (a través daquestes dades sabem directament qui és aquesta persona).
Dades d'identificació indirecta: adreça IP, correu electrònic, nacionalitat, dades de familiars, matrícula d'un vehicle (hi ha un registre de vehicles que permet conèixer el titular), sexe, color, raça, adreça postal, número de compte bancari, etc. .
És a dir, encara que la informació no identifiqui directament una persona (com pot ser el cas de la matrícula), es considera una dada de caràcter personal si mitjançant aquesta informació es pot arribar a identificar la persona sense esforç desproporcionat (podria acudir-hi al registre de vehicles i conèixer el titular de la matrícula, o acudir a l'adreça postal per veure qui hi viu).
No totes les dades tenen la mateixa importància. Dins les dades personals tenim **dades ESPECIALMENT PROTEGIDES o sensibles**, que tenen aquesta consideració per revelar circumstàncies o informació de les persones sobre la seva esfera més íntima i personal. **Per tant, REQUEREIXEN UNA ESPECIAL ATENCIÓ**. No és el mateix
conèixer l'adreça postal d'una persona que l'orientació sexual o les preferències polítiques o les dades de salut (per temes de discriminació i riscos).
Aquestes dades serien les que revelin origen ètnic o racial, opinions polítiques, conviccions religioses, filosòfiques, afiliació sindical, dades de salut, dades relatives a la vida sexual, orientació sexual, etc.
Cal tenir en compte **les DADES DE MENORS D'EDAT** (encara que no estiguin recollides en aquesta llista): als menors, se'ls considera un col·lectiu especialment vulnerable i per això les seves dades també han de ser tractades com si fossin especialment protegides. El Reglament els dedica un article expressament per a ells. **PER QUÈ?** Els nens mereixen una protecció específica de les vostres dades personals, perquè poden ser menys conscients dels riscos i conseqüències derivades del

tractament de les vostres dades personals.

• Què s'entén per tractament?

El tractament de dades consisteix en qualsevol activitat o qualsevol operació en què estiguin presents dades personals, independentment del mitjà utilitzat (automatitzat o no automatitzat)

Per exemple: La recollida de dades identificatives dels alumnes o familiars a la matrícula o fitxa del col·legi; carregar dades en plataformes del centre; publicar a les web fotos dels alumnes; consultar un informe sobre un alumne elaborat pel psicopedagog; fer els butlletins de notes; cedir dades a la Seguretat Social oa un Encarregat de tractament.

En definitiva, tot allò que suposi la recollida, registre, organització, modificació, consulta, supressió o destrucció de dades, entre d'altres (fins i tot agrupar els treballs fets per un alumne al llarg d'un curs).

• Què s'entén per bretxa de seguretat?

Qualsevol incidència que ocasioni la destrucció, la pèrdua, l'alteració, la modificació, o l'accés o la comunicació no autoritzats de dades personals. En definitiva, tot allò q afecti la confidencialitat, integritat o disponibilitat de les dades personals.

Exemples: enviament de correu electrònic amb informació confidencial a un destinatari erroni; la pèrdua d'exàmens; tenir coneixement que han entrat a la nostra sessió d'Alexia sense autorització; la pèrdua dun pen drive amb informació; virus informàtic que bloqueja les dades; accés no autoritzat per un alumne a l'ordinador d'un professor que conté qualificacions i altres dades dels alumnes; pèrdua/robatori de l'ordinador d'un docent on es guarda informació acadèmica dels alumnes.

En qualsevol cas, si tenim dubtes sobre si un incident pot constituir una bretxa de seguretat que afecti dades personals el correcte és sempre consultar a l'adreça del centre.

• Qui és el responsable del tractament?

Hem de distingir dues figures claus en el tractament de dades personals: d'una banda, el responsable del tractament i de l'altra, l'encarregat del tractament.

El Responsable del tractament és la persona física o jurídica que decideix sobre la finalitat i els mitjans del tractament de les dades personals. És a dir, és qui decideix per què (per què), com es tracten les dades i quines dades es tracten.

El Centre educatiu, com a Responsable del tractament, recull dades d'alumnes per prestar el servei educatiu/o recull dades dels seus empleats per gestionar el pagament de nòmines (donar compliment al contracte laboral), o dades bancàries per al pagament de l'any acadèmic.

El Centre com a Responsable del tractament decideix per què tracta les dades, quines dades tracta i com les tracta (a través de quins mitjans).

• Qui és l'encarregat del tractament?

Normalment són proveïdors de serveis externs. Són persones físiques o jurídiques que tracten dades per compte del responsable del tractament (sota les directrius del RT). La diferència rau que l'encarregat no decideix sobre finalitat (sobre per què i per a què es tracten les dades), ni decideix quines dades tracta.

Exemple: El centre és responsable de les dades personals dels empleats. Quan el centre transmet aquestes dades a un tercer/proveïdor (una assessoria) perquè aquest li presti un servei (fer-li les nòmines), aquest tercer actua com a Encarregat de tractament.

Altres exemples són les empreses d'activitats extraescolars, el servei de gestió informàtica, l'empresa de transports per a excursions, etc.

El centre és qui decideix sobre la finalitat i ús de les dades i sobre quines dades es tractaran.

Aquesta relació entre RT i ET s'ha de regular mitjançant la signatura d'un contracte d'accés a dades que regula quines dades se cedeixen, els drets i les obligacions, la durada de la cessió i la devolució de la informació.

• Què és el Delegat de Protecció de Dades?

És una figura que apareix a Espanya amb l'entrada del nou Reglament i que té caràcter obligatori per a certes entitats (entre les quals hi ha els Centres educatius).

Seria la persona dins l'organització que ha de complir les funcions de: Assessorament: informar i assessorar l'entitat.

Supervisió: supervisar el compliment de la normativa de privadesa Cooperació: cooperar amb l'autoritat de control competent (reclamacions)

Recomanació: davant de problemes amb una empresa per temes relacionats amb protecció de dades, acudir al seu Delegat de Protecció de Dades. Normalment la seva informació de contacte ha de constar a les polítiques de privadesa a la web.

2. Reglament General de Protecció de Dades

• Llei orgànica de protecció de dades i garantia dels drets digitals 3/2018.
• Normativa específica de cada sector. En el nostre cas, Llei orgànica 2/2006, de 3 de maig, deducació.
Aplicació del RGPD

El Reglament té efectes sobre tots els residents de la UE i sobre els tractaments de dades que tinguin efectes dins del territori de la UE.
A partir d'ara les empreses de fora de la UE no poden manifestar que la legislació no els és aplicable si estan brindant un servei que té efectes a la UE per mitjà del qual es tractin dades personals de residents de la UE.
Això és important ja que, amb el desenvolupament de les noves tecnologies, moltes de les empreses de programari que utilitzem per a programes educatius o serveis de cloud computing o computació al núvol (Google drive) són d'origen americà. En consideració, haurem d'estar alerta que aquestes empreses compleixin el que estableix l'RGPD.
Quin organisme s'encarrega a Espanya de vetllar pel compliment de la normativa de privadesa?
A Espanya tenim l'Agència Espanyola de Protecció de Dades (AEPD) com a autoritat de control independent que s'encarrega de vetllar pel compliment de la normativa. L'Agència té facultats d'inspecció i de sanció i he de dir que és l'organisme de control europeu que obre més procediments per vulneracions de la normativa, encara que les seves sancions no són les més altes.

3. Principis de protecció de dades.

El nou Reglament General de Protecció de Dades estableix certs principis amb què complir per realitzar el tractament de les dades personals.
• Licitud, lleialtat i transparència
Licitud vol dir que hem d'estar legitimats per tractar les dades, és a dir, que hi hagi una base jurídica que em permeti tractar les dades (per exemple, una Llei (Llei d'Educació, el consentiment o un contracte)).
Lleialtat: tractar les dades exclusivament per a la finalitat que he declarat a l'interessat (si sol·licito dades per prestar serveis educatius emparat a la Llei d'Educació, no puc després utilitzar aquestes dades per a finalitats publicitàries o màrqueting o de cessió a tercers).
Transparència: és a dir, que informem els interessats. A l'interessat li ha de quedar clar quines dades estem fent servir i per a què.
Això és molt important, **SEMPRE hem d'informar,** encara que no calgui obtenir el consentiment per al tractament.
Cal informar els interessats sobre:
a. Qui és el responsable del tractament (Centre educatiu).
b. Amb quina finalitat *seran* utilitzades les dades (exercir funcions educatives, prestar un servei, realitzar activitats extraescolars, gestionar els pagaments, etc).
c. Quina és la base legitimadora que permet el tractament de les dades (una obligació legal, executar un contracte…)
d. Quan temps seran conservats.
e. Si es preveu fer comunicació d'aquestes dades a altres persones. Per exemple, a un ET.
f. Quins drets tenen els interessats i com poden exercir-los.
g. La possibilitat de fer una denúncia davant una autoritat de control.
Aquesta informació ha de ser posada en coneixement dels interessats de manera prèvia a la recollida de les dades, o al mateix moment de recollida.
S'ha de proporcionar la informació de forma concisa, transparent i de fàcil accés (a la web, que no estigui més lluny de 2cliks), en llenguatge clar i senzill, especialment quan s'adreci a nens.
• Limitació de la finalitat
Les dades personals seran recollides per a fins determinats, explícits i legítims. Es tradueix que hem de ser clars en establir les finalitats del tractament, perquè l'interessat ha de saber amb claredat perquè utilitzaré les seves dades i per descomptat no utilitzar-les per a altres finalitats diferents de les indicades.
Si sol·licito dades per prestar serveis educatius emparat a la Llei d'Educació, no puc després utilitzar aquestes dades per a finalitats publicitàries o màrqueting o de cessió a tercers.
• Minimització de dades (adequades, pertinents i necessàries)
Implica que NO hem de demanar o sol·licitar més dades de les estrictament necessàries per al

compliment de les finalitats establertes prèviament. Si per prestar-te un servei només necessito el teu nom i correu electrònic, no he de sol·licitar la imatge o l'estat civil, per exemple.
i. Tinc instal·lades càmeres de videovigilància, no he de captar la via pública.
ii. Per avaluar-te o prestar-te una funció educativa, no necessitaré saber les teves idees polítiques o la teva orientació sexual.
iii. Per contractar-te com a docent, no necessito saber la matrícula del teu vehicle o si et trobes afiliat a algun sindicat.
Abans de demanar dades, ens hem de plantejar si realment les necessitem per a la finalitat perseguida.
• **Exactitud**
Ens obliga a mantenir les dades actualitzades, és a dir, a adoptar mesures raonables per esborrar o corregir les dades personals que siguin inexactes.
Què pot passar si no complim aquest principi? Per exemple, que enviem un correu electrònic amb informació sensible a un correu electrònic incorrecte (no actualitzat) i que la informació la rebi un tercer no autoritzat o que no sigui el destinatari real amb la conseqüent bretxa de seguretat.
També pot passar que per error haguem recollit que un alumne petit que es queda al menjador no té al·lèrgies alimentàries, i ingereixi un aliment que li provoqui una reacció.
• **Limitació del termini de conservació (cementiris de dades)**
Aquest principi ens diu que les dades han de ser conservades pel temps estrictament necessari per complir amb la finalitat per a la qual van ser recollides, i una vegada acabada aquesta finalitat per a la qual van ser demanades procedir al bloqueig i supressió.
Per quant de temps hem de conservar les dades una vegada acabada la finalitat per a la qual van ser recollides?
Aquí no hi ha uns terminis definits a la normativa de privadesa, per tant, haurem d'acudir a les normatives sectorials, Codi Civil, Llei d'Educació, Llei de Telecomunicacions, normativa laboral, blanqueig de capitals, normativa de videovigilància, etc.**evitar els cementiris de dades.** Conclosa la finalitat els bloquejo i quan acabin les possibles responsabilitats els esborro.
• **Responsabilitat proactiva**
Aquest principi estipula que **"no només cal complir, sinó que cal demostrar que estem complint".** La responsabilitat proactiva implica que s'apliquin mesures tècniques i organitzatives, no només per complir amb la normativa, sinó per demostrar-ne el compliment abans les autoritats. Concretament cal demostrar que complim els principis que acabem de veure. Com ho podem demostrar? Establint polítiques internes, signant compromisos confidencialitat, formant empleats, arxivant els formularis en què recaptem dades per si demana l'Agència, signant contractes d'accés a dades amb els proveïdors de serveis, etc.

4. Legitimació per al tractament.

El RGPD ens diu que, per poder tractar les dades personals, en el vostre cas dels ALUMNES o FAMILIARS, hem d'estar legitimats per alguna base jurídica que ens ho permeti.
El RGPD a l'article 6è estableix les bases legals que legitimen el tractament de les dades personals.
Aleshores podrem tractar dades (sent lícit el tractament) si es compleix almenys una de les condicions següents (és a dir, si es dóna alguna de les següents bases jurídiques/legitimació que ens empari per al tractament de dades). També se'n poden donar diverses en mateix tractament.
• **Compliment d'una obligació legal:** aquesta base s'aplica quan el tractament és necessari per complir una obligació legal aplicable al responsable del tractament.
Com a regla general la Llei Orgànica d'Educació legitima el tractament de les dades dels alumnes per a l'exercici de la FUNCIÓ EDUCATIVA. En aquest cas estaríem tractant les dades dels alumnes emparats per una obligació legal (les necessàries per exercir la funció educativa). L'EXEMPLE MÉS CLAR ÉS LES DADES D'ALUMNES I PARES A LA MATRÍCULA I A LA FITXA DE L'ALUMNE.
Un altre exemple de tractament de dades per obligació legal seria la cessió de les dades dels treballadors a la Seguretat Social, i aquest altre tipus de tractament "comunicació" de dades emparat per una norma legal (Llei General de la Seguretat Social).

• **Execució d'un contracte:** aquesta base legitima el tractament de dades quan és necessari per a l'execució d'un contracte on l'interessat és part o per a l'aplicació a petició de mesures precontractuals.
Exemple:
- El centre educatiu tracta dades del personal (dades identificatives i dades del compte bancari) per al pagament de la nòmina, emparant-se en el contracte laboral. També tracta el seu CV en els processos

de selecció (legitimant-se en aplicació de mesures precontractuals).
- El mateix passa amb les dades bancàries dels pares dels alumnes, que els tracto legitimant-me en l'execució d'un contracte de prestació de serveis.
• **Protecció d'interessos vitals:** estem davant d'una base jurídica que s'aplica quan el tractament és necessari per protegir interessos vitals de l'interessat o d'una altra persona física (recollida i cessió de dades de salut).
Exemple: si un alumne va tenir un accident o una reacció al·lèrgica, hem de tractar les seves dades de salut, oportunament recollides (primer tractament) pel centre, per saber com actuar en aquest cas o per comunicar-los (segon tractament) a l'entitat sanitària que va a tractar l'alumne. Recollida i cessió emparada per aquesta base.
• **Interès públic:** aquesta base de legitimació s'aplica quan el tractament és necessari per complir una missió realitzada en interès públic. Normalment aplica al tractament de dades que realitzen les administracions públiques com l'Agència Tributària (exemple), que està legitimada per interès públic a tractar les dades que contenen les declaracions de la renda dels contribuents per tal d'establir i verificar l'import dels seus impostos.
Quan el centre capta imatges per mitjà de càmeres de videovigilància, ho fa per salvaguardar la seguretat de les persones i dels seus béns, així com de les seves instal·lacions, i el centre està legitimat per l'interès públic per al tractament d'aquestes imatges.
• **Interès legítim:** ve a dir que el tractament de dades es pot realitzar si és necessari per a la satisfacció d'interessos legítims perseguits pel Responsable del tractament, sempre que sobre aquests interessos no prevalguin els interessos o els drets i les llibertats fonamentals de l'interessat que requereixin protecció de dades personals, en particular quan l'interessat sigui un nen. EXIGEIX PONDERACIÓ D'INTERESSOS.
No és un tema fàcil, a la realitat està subjecte a molta interpretació i és molt subjectiu.
Exemple: podríem dir que considerem que el Centre educatiu podria utilitzar, per exemple, el correu electrònic dels pares (una dada personal) per enviar publicitat sobre noves activitats ofertes pel col·legi, que es trobin al marge de la funció educativa.
• **Consentiment de l'interessat:** finalment, si no podem enquadrar el tractament de les dades personals en alguna de les bases de legitimació esmentades, cal sol·licitar el CONSENTIMENT dels interessats per al tractament de les seves dades.
Exemple més comú: el Centre educatiu vol prendre imatges dels alumnes per promocionar el col·legi i les seves activitats a la seva pàgina web oa les xarxes socials. Com que aquesta finalitat està fora de la funció educativa hem de prendre el consentiment.
El CONSENTIMENT s'ha d'obtenir amb caràcter previ a fer el tractament. És suficient que el consentiment s'obtingui una sola vegada, sense que sigui necessari renovar-lo, sempre que es mantingui la mateixa finalitat per a la qual es va demanar. És a dir, si et sol·licito el consentiment per publicar la teva imatge a la meva web, no tinc q renovar-lo cada any (tret que vulgui després publicar-la també en una altra plataforma). El consentiment, a partir de l'aplicació del nou RGPD, ha de ser atorgat a través duna clara acció afirmativa. No val dir "si no contestes aquest missatge o segueixes navegant pel meu web, entenc que atorgues el consentiment" = consentiment nul. CONSENTIMENT: "…tota manifestació lliure, especifica, informada i inequívoca per la qual l'interessat accepta, ja sigui mitjançant una declaració o una clara acció afirmativa, el tractament de dades personals que li concerneix…"
• **Consentiment Tractament de dades de menors**: per prestar el consentiment per al tractament de les vostres dades, cal que els alumnes tinguin més de 14 anys. Per a menors de 14 anys el consentiment ho han de donar els pares, tutors o representants legals.

5. **Menors – grups vulnerables** .

Els menors són considerats per la normativa com un grup especialment vulnerable, ja que són menys conscients dels riscos i les conseqüències que poden derivar-se del tractament de les seves dades personals.
Hem de tenir en compte que:
- El RGPD els dedica un article concret, exclusivament a ells.
- Les vostres dades no estan incloses dins de les dades especialment protegides que esmentem al principi, però s'han de tractar igual.
- L'AEPD hi posa el focus (per tant, als Centres educatius)
D'aquesta manera, hi ha una GRAN responsabilitat per al personal del Centre educatiu, no només pel que fa al TRACTAMENT de les dades dels alumnes, sinó, a CONSCIENCIAR els menors sobre les conseqüències del tractament de les dades personals.

Per això, els docents de l'Escola Quintanes han de:
- Fomentar el coneixement en matèria de protecció de dades.
- Educar en l'ús responsable dels mitjans telemàtics quan tracten dades personals (IPADE I ORDINADORS NOMÉS PER ÚS ESCOLAR).
- Conscienciar els menors que determinades conductes a la xarxa causen greus perjudicis.
- Contribuir a disminuir les situacions de risc.

• CANAL PRIORITARI AEPD

CANAL PER COMUNICAR A L'AEPD LA DIFUSIÓ DE CONTINGUT SENSIBLE PER INTERNET I SOL·LICITAR LA RETIRADA DE CONTINGUT SEXUAL O VIOLENT
És una de les grans iniciatives de l'AEPD que consisteix en una via ràpida i executiva per requerir a través de la pròpia Agència la retirada urgent de continguts especialment delicats que poguessin arribar a fer-se virals a les xarxes socials o internet.
Quan es pot fer servir el Canal Prioritari?
Parlem de continguts (fotografies o vídeos) de caràcter sexual o que mostrin actes d'agressió física o verbal.

- Agressions físiques i verbals, contingut sexual (els dos principals), però també imatges i vídeos que mostrin situacions d'assetjament, intimidació, humiliació, ofenses greus, discriminació o violència a altres alumnes o professors realitzades a través d'Internet, casos de sexting, ciberassetjament o ciberbullying.
-La clau és la immediatesa: aquest canal serveix per aturar la viralització del contingut, ja que la denúncia administrativa o penal o la via civil són molt lentes.
Qui pot activar el canal prioritari? Tant els afectats com qualsevol persona que tingui coneixement de la difusió d'aquest tipus de continguts.
Quan NO es pot fer servir el canal prioritari?
Quan la difusió s'estigui produint mitjançant serveis de missatgeria instantània (per exemple, WhatsApp o Telegram), o mitjançant correu electrònic.
En aquests casos, no és que no es pugui fer res, sinó que cal fer servir altres vies com la via ordinària (adreçar-se a la plataforma a través dels enllaços als formularis especials de les principals plataformes) o denunciar davant les Autoritats Competents.
Quina informació necessito aportar a l'AEPD per activar el canal prioritari efectivament?
Guardar evidències.
Enllaços web, perfils a RRSS del responsable, captures de pantalla, còpia de denúncia policial, còpia de sol·licituds de retirada a plataformes.
Què farà després l'AEPD?
Analitzarà la reclamació de forma prioritària i, si escau, ordenarà la retirada del contingut al prestador del servei o plataforma corresponent.
A més, si hi ha indicis de delicte, es dóna part a la fiscalia.

6. Responsabilitat.

Afecten als pares les actuacions realitzades pels fills menors d'edat?
En quines responsabilitats pot incórrer qui tracti o difongui il·legítimament continguts o informació sensible d'altres persones sense el seu consentiment?

- **Responsabilitat administrativa:** de la sanció econòmica per infracció a la normativa de protecció de dades imposada a menors d'edat majors de 14 anys responen solidàriament els seus pares, mares o tutors.

- **Responsabilitat civil:** els danys i perjudicis materials i morals causats a tercers per menors d'edat com a conseqüència d'aquestes conductes (delictives i no delictives) donen lloc a responsabilitat civil patrimonial, de què es fan càrrec els pares o tutors (solidària igual que en el cas anterior).

- **Responsabilitat penal:** els menors d'edat majors de 14 anys també responen pels delictes tipificats al Codi Penal com l'assetjament, les amenaces o el descobriment i la revelació de secrets, que s'apliquen als casos de sexting, ciberassetjament o ciberbullying.

- **Responsabilitat disciplinària en àmbit educatiu:** aquestes conductes donen lloc a responsabilitat disciplinària quan es produeixen als centres escolars (assetjament, intimidació, humiliació, ofenses greus, discriminació o violència a altres alumnes o professors realitzades a través d'Internet). Es poden imposar mesures correctives com l'amonestació verbal, l'advertència escrita o la suspensió del dret d'assistència al centre o l'expulsió de l'alumne o l'alumna.

7. Obligacions del personal docent i no docent.

• Conèixer la política de privadesa del Centre educatiu
La política de seguretat del centre en matèria de protecció de dades està pujada a internet. En aquesta política es troben descrites les mesures de seguretat adoptades pel centre per a la protecció de les dades personals i les obligacions en matèria de protecció de dades que heu de complir durant el desenvolupament de les vostres funcions laborals. És necessari i obligatori revisar aquesta política i comprometre's al seu compliment.
• Confidencialitat i Secret
Totes les persones (empleats i proveïdors) que accedeixin a dades de caràcter personal (dels alumnes o de les seves famílies) estan sotmeses al deure de guardar secret sobre aquesta informació.
A més d'aquest deure legal, és normal que els empleats es comprometin mitjançant la signatura d'un compromís de confidencialitat, on es reculli el deure de secret i confidencialitat i certes obligacions per assegurar la integritat i confidencialitat de les dades personals.
Per què el compromís de confidencialitat? En compliment del principi de responsabilitat proactiva, el centre no només ha de complir els principis establerts al Reglament sinó que ha de poder demostrar aquest compliment. Per això es desprèn la necessitat de fer signar aquest document (perquè pugui demostrar el centre que compleix el principi d'integritat i confidencialitat de la informació).
• Limitació del tractament
Només es podran utilitzar les dades personals dels alumnes o els seus pares o tutors per a les finalitats per a les quals van ser recollides, i aquestes són les finalitats comunicades als titulars
dades (ni una més ni una menys). No per exemple per enviar sol · licitud d'amistat per Facebook a un pare (cas real).
• Especial cura en l'ús d'aplicacions de missatgeria instantània
No crear grups amb els alumnes amb aplicacions de missatgeria instantània, sinó que cal emprar els mitjans i/o eines establertes pel Centre educatiu i posades a disposició d'alumnes i professors. En tot cas, utilitzar els correus electrònics.
En aquest tipus de grups es maneja una quantitat important de dades personals (de primera mà el nom i el número de mòbil de l'interessat, imatge, etc) i no sabem les mesures de seguretat que pren cadascun dels participants del grup per evitar l'accés tercers a aquest tipus d'aplicacions. Per això, l'accés duna persona no autoritzada podria generar un perjudici a tots els participants del grup.
Excepcionalment es podria crear un grup en el qual només constin les persones que han donat el seu consentiment per participar-hi (per a grups amb pares, no amb alumnes i on no es comparteixi informació personal dels alumnes, servint només per a coses com excursions o festivals).
• Captació d'imatges o enregistraments dels alumnes
No hem de prendre imatges o enregistraments dels alumnes per a finalitats alienes a la funció educativa.
En principi, només podem captar imatges d'alumnes per complir la finalitat educativa (cosa que poques vegades es donarà). Fora d'aquesta finalitat cal sol·licitar el consentiment dels menors o dels seus tutors legals.
Hem de donar compliment al principi de proporcionalitat i en la mesura que sigui possible no abusar de les imatges dels menors. Sempre és preferible utilitzar imatges on aquests no siguin reconeixibles (imatges llunyanes, d'esquena, de les mans dels alumnes treballant…)
Si fem fotos sense estar autoritzats pel centre, fora de la funció educativa o sense el consentiment ens convertirem en responsables en exclusiva d'aquest tractament de dades. Recordem les responsabilitats en què podem incórrer (administrativa, civil, penal i disciplinària),
Diferent seria el cas que la captació i l'enviament de la imatge sigui amb motiu que l'interès superior del menor estigués compromès, com en el cas d'algun accident o indisposició, i amb la finalitat d'informar i tranquil·litzar els pares se li enviï una foto del seu fill. En aquest cas existiria una base jurídica que legitima el tractament (compliment d'obligació legal d'informar els pares sobre l'estat del fill).
• Publicació de llistats dels alumnes
Hem d'evitar fer publicacions dels llistats dels alumnes (a parets de passadissos, portes, etc).
Poden existir situacions que fan necessària la publicació de llistats dels alumnes per gestionar

l'organització del centre.
Si és possible evitar-ho i gestionar-ho mitjançant l'aplicació que utilitzi el centre, a què tenen accés els alumnes, seria el correctíssim.
Si no és possible, que l'exposició de les llistes es limiti al temps estrictament raonable i necessari (i que es publiqui als llocs on, en principi, només hi poden accedir els interessats i que no estigui posat tot l'any).
Als menjadors dels alumnes es podran exposar els diferents menús, però sense necessitat que hi hagi un llistat amb nom i cognom dels alumnes en relació amb el menú que correspon a cada un. Aquesta informació sobre quin alumne correspon cada menú, per temes de salut i al·lèrgies, haurà d'estar en possessió del centre o de la persona autoritzada.

• **Utilització d'aplicacions/plataformes educatives**

La utilització d'aplicacions educatives per part dels professors o alumnes, on es tractin dades personals, només serà possible amb l'autorització expressa prèvia del centre.

El centre haurà de dur a terme una avaluació de l'aplicació des del punt de vista de la seguretat de la informació (si teniu política, quines dades tracta, identitat del responsable, transferències internacionals, possibilitat d'exercir drets, amb quina finalitat tracta les dades, etc).
Un cop feta aquesta avaluació, s'atorgarà l'autorització o la denegació per part del centre.
Si escau, el centre haurà d'informar els pares o tutors del començament de la utilització de la tecnologia a les aules, així com de les aplicacions que tractin dades personals dels alumnes i la seva funcionalitat.

• **Notificació de qualsevol incidència o violació de la seguretat de les dades personals**

Si tenim coneixement que s'ha produït una incidència amb relació al tractament de les dades personals, ho hem de comunicar al centre o al seu DPO.
S'entén per violació de la seguretat de les dades personals tot acte que ocasioni la destrucció, pèrdua o alteració accidental o il·lícita de dades personals o la comunicació o accés no autoritzat, així com la manca de disponibilitat de les dades.
Exemple: tenim coneixement que una persona no autoritzada ha tingut accés a dades personals dels alumnes o hem extraviat un pen drive on tenim dades personals dels alumnes. Hem de comunicar-ho immediatament al Responsable del tractament.
El nou RGPD estableix l'obligació per al responsable del tractament de notificar qualsevol violació de la seguretat de les dades personals tractades (72 hores). En cas de no fer-ho, s'imposarà una multa a aquest.
El centre ha desenvolupat un document de seguretat on es detalla com cal procedir en aquest tipus de casos, així com un protocol per a violacions de seguretat.

• **Salvaguarda de la contrasenya**

Les contrasenyes són una mesura de seguretat bàsica i fonamental en el tractament de dades que permet que només les persones autoritzades tinguin accés a les dades personals tractades.
Cada usuari serà responsable de la confidencialitat de les contrasenyes que se li assigni per accedir a dades personals i, en cas que aquesta sigui coneguda, fortuïta o fraudulentament, per persones no autoritzades, haurà de registrar-la com una violació a la seguretat de les dades personals i procedir al canvi.
Hem de triar contrasenyes segures, és a dir, contrasenyes robustes que evitin es descobertes.
Cal triar contrasenyes amb almenys 8 caràcters i de tipus alfanumèric. Evitar contrasenyes senzilles.
- 1234 no és una contrasenya.
- La paraula "contrasenya" no és una contrasenya.

8. Obligacions bàsiques.

a. No exhibir dades personals de manera directa o indirecta a persones no autoritzades.
- No comentar amb companys.
- Enviament de correus electrònics en còpia oculta.
- Revisar els destinataris (per exemple, en l'enviament de correus a famílies).

b. Impedir que durant el tractament de dades personals persones alienes puguin tenir-hi accés.

- Política de taules netes.
- Guardar la informació en armaris, sales tancades amb claus.
- Protectors de pantalla

- Impressores compartides: en cas d'utilització d'impressores, assegureu-vos que no quedin documents impresos a la safata de sortida.

c. Rebutjar de forma segura els suports d'informació.

- Quan utilitzem suports en paper, el correctíssim seria utilitzar destructores de paper, sinó a mà. Quan utilitzem discs durs, pen drives o CD, realitzar-ne un format segur.

d. Protegir la informació fora de làmbit corporatiu.

- Especial cura al robatori o pèrdua dels suports o equips utilitzats.
- Com a mesura es pot adoptar el xifratge de qualsevol suport que surti del Centre educatiu o tancar la sessió d'inici tant al dispositiu com a les plataformes.-
- No utilitzar el desament automàtic de contrasenyes.

9. Bretxes de seguretat.

Qualsevol incidència que ocasioni la destrucció, la pèrdua, l'alteració, o l'accés o la comunicació no autoritzats de dades personals, així com el bloqueig de la informació. En definitiva, tot allò que afecti la confidencialitat, integritat o disponibilitat de les dades personals. És a dir, que a la dada hi accedeixin persones no autoritzades, que la dada sigui modificada o que no es pugui accedir a la informació.
Quan es produeix una violació de seguretat hem de tenir en compte dues coses:
- pot ser necessari comunicar-ho a les persones afectades.
- Pot ser necessari comunicar-ho a l'utoritat de control competent.

Hi ha excepcions a aquesta comunicació: seria el cas en què es prevegi q la incidència no pugui suposar un risc per als afectats (perquè haguem establert mesures de seguretat adequades i sigui improbable que es produeixi un dany). Per això serà important tenir en compte els terminis, la comunicació s'haurà de fer sense dilació indeguda i com a màxim en un termini de 72 h.
En qualsevol cas, si tenim dubtes sobre si un incident pot constituir una bretxa de seguretat que afecti dades personals el correcte és sempre consultar a l'adreça del centre.
Comunicar una bretxa no suposa que ens sancionin, en canvi, si no la comuniquem si és altament probable que ens sancionin.

10. Drets dels interessats.

En què consisteix cada dret?

Dret d'accés: dret a conèixer quines dades personals disposa l'empresa sobre mi, juntament amb la finalitat per a la qual han estat recollits, la categoria de dades personals que es tracten, la identitat dels destinataris de les dades, els terminis de conservació, i la identitat del responsable.
Dret de rectificació: dret que es rectifiquin aquelles dades inexactes o incompletes.
El **dret d'oposició**, com el seu nom indica, suposa l'oposició que el responsable realitzi un tractament de les dades personals. Per exemple, oposar-me a l'enviament de publicitat comercial.
Dret de supressió suposa l'esborrament de les dades quan no hi hagi una obligació o deure legal que ho impedeixi.
No es procedirà a l'esborrament físic de les dades sinó al seu **"bloqueig"** apartant-los de qualsevol procés o tractament fins que vencen els terminis legals de prescripció de les responsabilitats derivades del tractament.
Exercici del dret de portabilitat: aquí un exemple clar és quan canviem de companyia telefònica, ja que sol·licitarem a un Responsable del tractament que comuniqui les nostres dades a un altre Responsable del tractament.
Dret a la limitació del tractament: aquest dret és una mena de mesura cautelar. Puc sol·licitar a una entitat que deixi de tractar les meves dades mentre s'està resolent, per exemple, una sol·licitud de rectificació de dades o mentre es resol un litigi legal que mantinc amb la entitat.
Característiques comunes a aquests drets.
- Són personalíssims, és a dir, només els pot exercir l'interessat o un representant legal.
- S'ha de donar resposta sense dilació indeguda i en un termini màxim d'un mes.

16
- L'exercici de qualsevol és gratuït amb caràcter general.
- Són independents, és a dir, els puc exercir indistintament.
En cas que rebem una comunicació en què se sol·licités l'exercici dels drets de accés, rectificació, supressió, limitació, oposició i/o portabilitat, **hem de posar-ho immediatament en coneixement de la persona responsable** (Centre).

11. RESUM.

- **Dada personal: informació que identifiqui o faci identificable una persona.**
- **Tractament: qualsevol activitat sobre les dades personals independentment del medi (automatitzat o no).**
- **Responsable i encarregat: La diferència, el responsable és el que decideix sobre la finalitat.**
- **Consentiment: s'ha d'atorgar mitjançant una declaració o una clara acció afirmativa.**
- **Proactivitat: demostrar que complim amb els principis del Reglament abans i durant el tractament de les dades.**
- **Drets: important, donar resposta sense dilació indeguda i en el termini màxim d'un mes.**
- **Mesures tècniques i organitzatives: garantir la confidencialitat, integritat i disponibilitat.**
- **Violacions de seguretat: qualsevol incident q pugui afectar la confidencialitat, integritat o disponibilitat de les dades persones.**
- **Comunicar-ho a l'AEPD sense dilació indeguda i en el termini màxim de 72 hores.**
- **AEPD: Agència Espanyola de Protecció de Dades com a autoritat de control encarregada de vetllar pel compliment de la normativa de privadesa a Espanya**