

DIDATTICA DIGITALE

E-LEARNING NELLA SCUOLA

SCUOLA POLO PER LA FORMAZIONE – AMBITO TERRITORIALE 07

Formazione Docenti – Privacy

dott.ssa Daniela Cotzia - d.cotzia@knowk.it



Know K. è agenzia accreditata dal MIUR per la formazione del personale della scuola Secondo Direttiva Ministeriale n.170/2016 (ex n. 90/2003).



Know K. è azienda certificata ISO 9001-2015 per la qualità dall'anno 2000, sulla progettazione ed erogazione della formazione.

La Privacy



Argomenti del Corso

- Le nuove disposizioni normative
- Il trattamento dei dati personali
- La protezione dei dati personali a scuola

La privacy

La Privacy è il diritto alla riservatezza della propria vita privata ed include:

- **Dati anagrafici**, nome, cognome e indirizzo mail, indirizzo di residenza e/o domicilio, numero di telefono, ecc.
- **Dati finanziari**, codice fiscale, conto corrente, numero carta di credito ecc.
- **Dati sensibili**, informazioni utili a ricavare nazionalità, opinioni politiche, convinzioni religiose, ecc.
- **Dati giudiziari**, processi, denunce ecc.



Quali sono i dati da proteggere

Dati Personali

- Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Quali sono i dati da proteggere

Dati Sensibili

- I dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Quali sono i dati da proteggere

Dati Giudiziari

- I dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti.

Cosa significa trattare i dati

Il Codice per la tutela della Privacy prevede **che i dati siano:**

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi siano raccolti o successivamente trattati.

Chi può trattare i dati personali

Relativamente alla comunicazione dei dati da parte dei soggetti pubblici, il **Codice prevede che:**

- La comunicazione da soggetto a soggetto pubblico è ammessa se prevista da una norma di legge/di regolamento o in mancanza, ove necessaria per lo svolgimento di funzioni istituzionali;
- La comunicazione/diffusione da soggetto a privati/a enti pubblici economici, è ammessa solo ove prevista da una norma di legge/di regolamento..

Chi è il titolare del Trattamento dei dati

E' la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine a:

- Le finalità perseguite;
- Le modalità del trattamento dei dati personali;
- Gli strumenti utilizzati;

Chi è il Referente Responsabile del Trattamento dei dati

- E' la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che **siano preposti dal titolare al trattamento di dati personali.**

Chi è l'incaricato del Trattamento

- E' la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal referente.
- La designazione è effettuata per iscritto e individua l'ambito del trattamento consentito.

Misure minime: Allegato B

- Ridurre al minimo i rischi: i dati personali devono essere custoditi con cura e controllati;
- I rischi sono: la distruzione, la dispersione, il trattamento illecito;
- L'allegato B descrive le misure minime per ridurre il rischio.

Autenticazione informatica

- E' un codice di identificazione dell'incaricato + una parola chiave riservata oppure una caratteristica biometrica + una parola chiave;
- Ogni incaricato può avere uno o più codici di autenticazione;
- L'incaricato è obbligato a custodire ed assicurare la segretezza della parola chiave (niente più post-it appiccicati sul monitor);
- L'incaricato non lascia sessioni aperte incustodite

Autenticazione informatica

La parola chiave:

- Deve avere almeno 8 caratteri;
- Non deve contenere riferimenti all'incaricato;
- Una volta ricevuta l'incaricato la cambia;
- Scade al più ogni sei mesi (consigl. 3 mesi);
- Non può essere ceduta ad altri;

Autenticazione informatica

Assenza dell'incaricato

- In caso di prolungata assenza dell'incaricato il Responsabile del trattamento preleva la parola chiave dalla busta sigillata e la consegna a colui che dovrà operare sullo strumento elettronico;
- L'incaricato al suo rientro sarà costretto all'immediato cambio della parola chiave con successiva consegna al responsabile del trattamento per la custodia;

Sistema di autorizzazione

- Periodicamente (almeno annualmente) il profilo di autorizzazione va verificato nella sua sussistenza;
- Vanno eliminate le credenziali non usate da più di sei mesi

Trattamento di dati sensibili e giudiziari

- I supporti di copia dei dati e i supporti rimovibili vanno protetti contro l'accesso abusivo (ad es. in cassaforte);
- Il trasporto elettronico dei dati sensibili e giudiziari deve essere cifrato.

Archivi cartacei

- Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento dei dati personali;
- In caso di atti contenenti dati sensibili e giudiziari, questi ultimi vanno controllati e custoditi dall'incaricato durante tutto il trattamento fino alla restituzione in archivio;
- Il documento delineante le funzioni relative al trattamento dei dati che l'incaricato riceve può anche essere redatto per classi omogenee di incarico.

Adempimenti periodici

1° gennaio di ogni anno:

- Aggiornare l'individuazione dell'ambito di trattamento consentito agli incaricati;
- Verificare la sussistenza delle condizioni di autorizzazione;
- Programmare gli eventi formativi per gli incaricati;
- Aggiornare il SW antivirus/firewall, "patch" dei programmi (attività da ripetere anche il 1° luglio di ogni anno)

Documento Programmatico della Sicurezza

Entro il 31 marzo di ogni anno il Titolare ed il Responsabile del Trattamento redigono un aggiornamento del DPS; che contiene:

- L'elenco dei trattamenti di dati personali;
- La distribuzione dei compiti e delle responsabilità;
- Le misure adottate per garantire disponibilità ed integrità dei dati;
- Criteri e modalità di ripristino dei dati;
- Misure di sicurezza per dati affidati all'esterno della struttura;
- Gli interventi formativi degli incaricati.

GDPR (General Data Protection Regulation)

Regolamento UE 2016/679



GDPR (General Data Protection Regulation)

Regolamento UE 2016/679

- E' il regime di protezione dei dati personali proposto dalla C.E. per tutti gli stati membri;
- È stato adottato il 27 aprile 2016;
- È andato in vigore dal 25 maggio 2018;
- Non è una direttiva e quindi non ha bisogno di alcuna legislazione applicativa degli stati membri;

GDPR (General Data Protection Regulation)

Regolamento UE 2016/679

- Sono obbligati ad attenersi al regolamento anche entità che non fanno parte della C.E., ma che hanno dati residenti nei territori degli stati membri della C.E.
- Il regolamento non riguarda la gestione di dati personali per attività di sicurezza nazionale o di ordine pubblico.

GDPR (General Data Protection Regulation)

Regolamento UE 2016/679

- Ogni stato membro dovrà istituire un'autorità per sovrintendere i reclami, le indagini e sanzionare le infrazioni sul trattamento dei dati personali.
- Una commissione europea per la protezione dei dati (EDPB, European Data Protection Board) coordinerà le autorità sovrintendenti degli stati membri.

GDPR (General Data Protection Regulation)

Regolamento UE 2016/679

Le Responsabilità:

- Le notifiche sul trattamento dei dati dovranno includere il tempo di mantenimento dei dati;
- Si dovrà comunicare chi controlla i dati e chi protegge i dati;
- Si avrà diritto a contestare le decisioni automatizzate, compresa la profilazione, oggetto di elaborazione algoritmica;
- Non sono inclusi i dati personali necessari ed essenziali per dare vita ad un rapporto contrattuale;

GDPR (General Data Protection Regulation)

Regolamento UE 2016/679

Una novità sul trattamento:

- Il regolamento specifica anche il caso del trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale.
- Prevede pertanto che l'interessato venga prontamente informato in presenza di una violazione sul trattamento dei dati, che metta a rischio i suoi diritti e le sue libertà.

GDPR (General Data Protection Regulation)

Regolamento UE 2016/679

Il “Data Breach” (violazione di dati personali)

- Il titolare del trattamento dei dati avrà l'obbligo legale di comunicare le fughe di dati all'autorità nazionale.
- Le denunce di fughe di dati devono essere trasmesse all'autorità sovrintendente non appena se ne viene a conoscenza e comunque entro 72 ore dall'evento.
- In alcune situazioni le persone di cui sono stati sottratti i dati dovranno essere avvertite.

GDPR (General Data Protection Regulation)

Regolamento UE 2016/679

Diritto all'oblio

- Il cosiddetto “diritto all'oblio” è il diritto alla cancellazione, limitazione e rettifica dei dati personali e stabilisce che il soggetto ha il diritto di richiedere la cancellazione dei suoi dati personali in caso di mancata osservanza delle norme;
- L'interessato deve poter esercitare questo suo diritto con la stessa facilità con cui ha espresso il consenso al trattamento dei suoi dati.

GDPR (General Data Protection Regulation)

Regolamento UE 2016/679

Diritto all'oblio

- Il responsabile del trattamento, dietro richiesta dell'interessato, gli dovrà comunicare i destinatari a cui ha trasmesso la sua richiesta di cancellazione.
- Sul responsabile del trattamento grava lo stesso onere in caso di richiesta di limitazione o di rettifica dei dati presentata dall'interessato.

GDPR (General Data Protection Regulation)

Regolamento UE 2016/679

Portabilità dei dati:

- Una persona deve essere in grado di trasferire i propri dati personali da un sistema di elaborazione elettronico a un altro senza che il controllore dei dati possa impedirlo.

La Privacy a Scuola



Temi in Classe

- **Non lede la privacy** l'insegnante che assegna ai propri alunni lo svolgimento di **temi in classe riguardanti il loro mondo personale.**
- Sta invece nella sensibilità dell'insegnante, nel momento in cui gli elaborati **vengono letti in classe, trovare l'equilibrio tra esigenze didattiche e tutela della riservatezza,** specialmente se si tratta di argomenti delicati.



Cellulari e Tablet

- **L'uso di cellulari e smartphone è in genere consentito** per obiettivi finalizzati allo studio o per registrare lezioni
- **Spetta comunque agli istituti scolastici decidere nella loro autonomia come regolamentare** o se vietare del tutto l'uso dei cellulari
- **Non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese.** E' bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati
- **Stesse cautele vanno previste per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi online**

Recite e gite scolastiche

- **Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici**
- **Le immagini in questi casi sono raccolte a fini personali e destinati ad un ambito familiare o amicale.** Nel caso si intendesse pubblicarle e diffonderle in rete, anche sui social network, è necessario ottenere di regola il consenso delle persone presenti nei video o nelle foto.



Retta e servizio mensa

- **E' illecito pubblicare sul sito della scuola il nome e cognome degli studenti i cui genitori sono in ritardo nel pagamento della retta o del servizio mensa**
- **E' illecito pubblicare sul sito della scuola il nome e cognome degli studenti che usufruiscono gratuitamente del servizio mensa in quanto appartenenti a famiglie con reddito minimo o a fasce deboli**
- **Gli avvisi messi on line devono avere carattere generale, mentre alle singole persone ci si deve rivolgere con comunicazioni di carattere individuale**
- **A salvaguardia della trasparenza sulla gestione delle risorse scolastiche, restano ferme le regole sull'accesso ai documenti amministrativi da parte delle persone interessate**



Telecamere

- Si possono in generale installare **telecamere all'interno degli istituti scolastici**, ma **devono funzionare solo negli orari di chiusura degli istituti e la loro presenza deve essere segnalata con cartelli**
- Se le riprese riguardano **l'esterno della scuola**, **l'angolo visuale delle telecamere deve essere opportunamente delimitato**
- Le immagini registrate devono essere cancellate, in generale, dopo **24 ore**



Inserimento professionale

Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale le scuole, **su richiesta degli studenti, possono comunicare e diffondere alle aziende private e alle pubbliche amministrazioni i dati personali dei ragazzi**



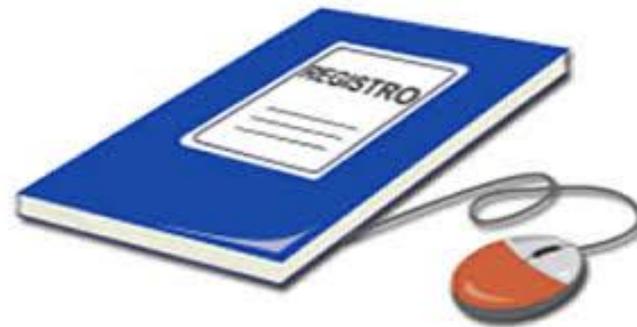
Questionari per attività di ricerca

- **L'attività di ricerca con la raccolta di informazioni personali tramite questionari da sottoporre agli studenti è consentita solo se ragazzi e genitori sono stati prima informati sugli scopi delle ricerca, le modalità del trattamento e le misure di sicurezza adottate**
- **Gli studenti e i genitori devono essere lasciati liberi di non aderire all'iniziativa**



Iscrizione e registri on line, pagella elettronica

- In attesa di poter esprimere il previsto parere sui provvedimenti attuativi del Ministero dell'istruzione riguardo all'iscrizione on line degli studenti, all'adozione dei registri on line e alla consultazione della pagella via web, il **Garante auspica l'adozione di adeguate misure di sicurezza a protezione dei dati.**



Voti, scrutini, esami di Stato

- **I voti dei compiti in classe e delle interrogazioni, gli esiti degli scrutini o degli esami di Stato sono pubblici.** Le informazioni sul rendimento scolastico sono soggette ad un regime di trasparenza e il regime della loro conoscibilità è stabilito dal Ministero dell'istruzione.
- **E' necessario però, nel pubblicare voti degli scrutini e degli esami nei tabelloni, che l'istituto eviti di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti: il riferimento alle "prove differenziate" sostenute dagli studenti portatori di handicap, ad esempio, non va inserito nei tabelloni, ma deve essere indicato solamente nell'attestazione da rilasciare allo studente.**

Trattamento dei dati personali

- **Le scuole devono rendere noto alle famiglie e ai ragazzi, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano**
- Spesso le scuole utilizzano nella loro attività quotidiana **dati sensibili** - come quelli **riguardanti le origini etniche, le convinzioni religiose, lo stato di salute** - anche per fornire semplici servizi, come ad esempio la mensa. E' bene ricordare che **nel trattare queste categorie di informazioni gli istituti scolastici devono porre estrema cautela, in conformità al regolamento sui dati sensibili adottato dal Ministero dell'istruzione**
- **Famiglie e studenti hanno diritto** di conoscere quali informazioni sono trattate dall'istituto scolastico, farle **rettificare se inesatte, incomplete o non aggiornate**