ESPOSTO ALL'ALBO DELLA SCUOLA NEGRELLI E GANDHI

IL 29.01.2015

ISTITUTO COMPRENSIVO ROVERETO NORD

PRIVACY E TUTELA DELLA DIGNITÀ

ISTRUZIONI OPERATIVE

per garantire la corretta gestione dei dati personali

La tutela della riservatezza e il diritto di ciascuno di non dover subire invasioni nella propria sfera privata sono ormai entrati a far parte della nostra vita quotidiana. Siamo però immersi in una società che non può astenersi dal trattare dati personali, soprattutto al fine di fornire beni o servizi. Le informazioni vengono raccolte, elaborate, comunicate ad altri soggetti, anche tramite reti di comunicazione elettronica. Si è quindi ravvisata la necessità di tutelare sia l'identità personale che i dati personali.

Il Codice in materia di protezione dei dati personali (decreto legislativo 196/03), rappresentando una raccolta organica e sistematica delle norme sulla privacy, è finalizzato a disciplinare un settore delicato come la tutela dei diritti, delle libertà fondamentali, della dignità della persona, definendo regole generali e specifiche al fine di un corretto e trasparente trattamento dei dati raccolti.

Concetto fondamentale del Codice è il diritto alla protezione dei dati personali. Questo diritto viene tutelato sia con misure di tipo preventivo (quali ad esempio l'informativa all'interessato o le misure di sicurezza), sia di tipo successivo (quali ad esempio il controllo che può esercitare l'interessato sui propri dati o le sanzioni previste).

Anche l'istituzione scolastica è tenuta a garantire la tutela del diritto alla riservatezza dei soggetti con cui entra in contatto (alunni, famiglie, personale, ecc.) mediante idonee procedure.

Il presente opuscolo mira ad informare e sensibilizzare tutti coloro che operano nel nostro contesto scolastico sulle disposizioni previste dalla legge di riferimento e sui rischi che può comportare il trattamento di dati personali.

GUIDA OPERATIVA PER GLI INCARICATI DEL TRATTAMENTO

DEFINIZIONI

Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

Dato personale: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

Dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato;

Dati sensibili : i dati personali 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;

Dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Titolare: 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 alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

Responsabile: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

Interessato: la persona fisica cui si riferiscono i dati personali;

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

PRINCIPI GENERALI

L'art. 11 specifica le regole generali alle quali devono essere adeguati tutti i trattamenti di dati. Secondo tali principi ogni trattamento deve essere lecito e corretto; la nozione di liceità comporta ontologicamente che il trattamento debba essere eseguito sia nel rispetto delle disposizioni specifiche di legge previste dalla normativa a carattere speciale sia nel rispetto dei principi generali del diritto; la correttezza si riferisce a regole di condotta non giuridiche da applicarsi al trattamento di dati personali. Inoltre i dati devono essere raccolti e registrati per scopi determinati, espliciti e legittimi; questo significa che, prima dell'inizio del trattamento, si devono determinare le finalità per le quali i dati vengono raccolti e trattati, limitando la raccolta delle informazioni a quei dati che siano strumentali e funzionali allo scopo del trattamento, informandone l'interessato il quale potrà esercitare i propri diritti sui propri dati personali; i dati raccolti dovranno quindi essere esatti e, se necessario, aggiornati nonché pertinenti, completi e non eccedenti; risulta quindi necessario procedere ad un iniziale controllo in fase di raccolta dei dati al fine di evitare di raccogliere dati non necessari allo scopo del trattamento pur nella loro completezza al fine di avere un quadro completo dell'interessato in relazione al trattamento effettuato, seguito da periodiche verifiche al fine di aggiornare, se necessario, i dati.
Infine i dati devono essere conservati per un periodo non superiore a quello necessario allo scopo per il quale sono stati raccolti. E' quindi necessario valutare se e per quanto tempo la normativa di riferimento preveda la conservazione dei dati, tenendo presente la normativa contabile e fiscale, nonché la conservazione della documentazione per fini storici, statistici o scientifici, con particolare attenzione alla normativa archivistica.

INFORMATIVA DELL'INTERESSATO

L'articolo 13 del Codice prevede che l'interessato sia informato in merito all' identità del soggetto che ha intenzione di trattare i dati personali dell'interessato stesso e in merito all'utilizzo che ne verrà fatto. Scopo di questo adempimento è consentire all'interessato di poter seguire le informazioni a lui riferite ed eventualmente esercitare i diritti conferitigli dal Codice.
In particolare la normativa prevede che l'interessato o la persona presso cui sono raccolti i dati debba essere previamente informato oralmente o per iscritto circa:

- Finalità e modalità del trattamento cui sono destinati i dati;
- La natura obbligatoria o facoltativa del conferimento dei dati;
- Le conseguenze di un eventuale rifiuto di rispondere;
- I soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati;
- L'ambito di diffusione dei dati;
- Gli estremi identificativi del titolare e del responsabile.

Nel caso in cui, poi, i dati siano di tipo sensibile o giudiziario, deve essere inserito il riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento di tali dati. Se i dati non sono raccolti direttamente presso l'interessato ma sono raccolti presso terzi, l'informativa all'interessato può essere data all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione. In questo caso devono essere comprese nell'informativa le categorie di dati trattati. Questa disposizione non si applica se i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria, se i dati sono trattati ai fini dello svolgimento delle investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria oppure su concessione del Garante.

ADEMPIMENTI PER GLI INCARICATI
Per una corretta applicazione di queste norme è necessario che gli incaricati, al momento della raccolta dei dati, provvedano a tali adempimenti:

- fornire l'informativa relativa al trattamento dei dati così come predisposta dal titolare del trattamento eventualmente integrandola nelle parti di competenza;
- verificare l'esattezza, la pertinenza e la completezza dei dati trattati;
- non raccogliere più dati del necessario;
- rispettare l'obbligo di riservatezza e segretezza in relazione ai dati di cui si viene a conoscenza;
- far rispettare la distanza di cortesia nei rapporti di tipo front-office al fine di garantire la riservatezza e la discrezione nel trattamento e nella comunicazione dei dati.

DIRITTI DEGLI INTERESSATI
L'articolo 7 del Codice conferisce all'interessato il diritto di accesso ai propri dati personali e altri diritti.
In particolare l'interessato ha diritto di:

1. Ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. Ottenere l'indicazione:

a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati

3. Ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. Opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Questi diritti possono essere esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato; alla richiesta è fornito idoneo riscontro senza ritardo.
La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Quando riguarda l'esercizio dei diritti previsti al punto 1 e 2 dell'elenco precedente, la richiesta può essere formulata anche oralmente e in tal caso deve essere annotata sinteticamente a cura dell'incaricato o del responsabile. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia. Nel caso in cui sia effettuata una richiesta in tal senso, il responsabile o gli incaricati devono estrarre i dati e comunicarli al richiedente. I dati possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare.

RISCHI CHE INCOMBONO SUI DATI E MISURE DI SICUREZZA
Il codice privacy prevede l'adozione di misure di sicurezza idonee e preventive in modo tale da ridurre al minimo i rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, tenendo conto del progresso tecnico, della natura dei dati trattati e delle specificità dei trattamenti.
Il titolare del trattamento deve quindi, anche attraverso la collaborazione del responsabile, se nominato, e degli incaricati provvedere a mettere in atto tutte le misure di sicurezza a protezione dei dati personali trattati.
In particolare il codice individua alcune misure di sicurezza, definite "minime", volte ad assicurare un livello minimo di protezione dei dati personali.
In questa sezione vengono evidenziati i principali rischi che possono incombere sui dati e le misure di sicurezza adottate a disposizione degli incaricati. La puntuale applicazione e il corretto utilizzo di tali misure da parte degli incaricati sono condizione essenziale per una sicurezza dei dati.

TRATTAMENTI CON STRUMENTI ELETTRONICI

Protezione dei dati da accessi non consentiti o trattamenti non autorizzati
Ogni utente deve essere dotato di credenziali di autenticazione consistenti in un codice per l'identificazione dell'incaricato (nome utente) e una password oppure in un dispositivo di autenticazione in possesso ed uso esclusivo dell'incaricato oppure in una caratteristica biometrica dell'incaricato, eventualmente associati ad un codice identificativo o ad una password, in modo tale che solo gli incaricati dotati di tali credenziali di autenticazione possano accedere a uno specifico trattamento o insieme di trattamenti attraverso il superamento di un'idonea procedura di identificazione. Questa misura di sicurezza protegge i dati da accessi non autorizzati. E' obbligatorio che la password che compone le credenziali di autenticazione sia mantenuta segreta dalla persona a cui è assegnata. Infatti una divulgazione a terzi di tale password comprometterebbe la sicurezza dei dati permettendo un accesso abusivo ad essi da parte di persone non autorizzate.
Altre misure di sicurezza riguardano l'obbligo di modifica della password da parte dell'utente del sistema informatico al primo utilizzo e successivamente ogni tre mesi (nel caso di trattamento di dati sensibili o giudiziari) o sei mesi in caso di trattamento di dati comuni, la lunghezza della password e il divieto di utilizzare riferimenti agevolmente riconducibili all'incaricato. Tale obbligo ha la funzione di proteggere sia i dati personali trattati (un soggetto estraneo che si introduca nel sistema potrebbe modificare o cancellare i dati contenuti), sia l'incaricato stesso che utilizza la password (in caso di accesso ai dati tramite la password dell'utente, il sistema registra l'accesso attribuendolo all'utente stesso).
L'associazione di una password non facilmente riconducibile all'incaricato (ad esempio è vietato indicare il proprio nome o cognome, quello dei familiari o la data di nascita e tantomeno utilizzare il nome utente), unita ad una lunghezza adeguata e il suo cambiamento in tempi ragionevolmente brevi permette di contrastare accessi abusivi al sistema informatico o eventuali tentativi di scoprire o sottrarre, anche con modalità informatiche, la password utilizzata.
Nel caso in cui siano utilizzati come credenziali di autenticazione al posto di codice identificativo (nome utente) e password, dispositivi di autenticazione (ad esempio smart card) eventualmente associate ad una password, fermo restando quanto già indicato per la password, è necessario che la persone in possesso di tali dispositivi di autenticazione si preoccupino di conservarli con cura, non cedendoli a terzi né lasciandoli a disposizione di terzi. (ad esempio non lasciare questi dispositivi a disposizione di chiunque sulla scrivania o posto di lavoro).
La collaborazione degli utenti del sistema informatico è richiesta anche in relazione alla custodia degli strumenti elettronici. In particolare è misura minima di sicurezza provvedere a non permettere che terzi non autorizzati utilizzino gli strumenti informatici in assenza dell'incaricato. A tal fine è obbligatorio che al termine dell'orario lavorativo il PC in dotazione venga spento. E' inoltre previsto che, in caso di assenza temporanea dalla propria postazione (ad esempio

nelle pause pranzo, o in caso di allontanamento in genere) si provveda a bloccare la possibilità di utilizzo. A tal fine sono possibili varie soluzioni quali spegnere il PC o chiudere la porta a chiave.
La soluzione più immediata e facilmente adottabile rimane comunque quella di bloccare il PC (ctrl + alt + canc – blocca computer). In tal modo solo inserendo la password di accesso sarà possibile accedere ai dati ripartendo esattamente dal punto lasciato in sospeso. Altra soluzione possibile è attivare la procedura di screen saver con password: in caso di non utilizzo del sistema, a cadenza prestabilita, si attiverà lo screen saver obbligando l'utente all'inserimento della password.
E' possibile che talora sia necessario accedere ai dati in assenza dell'incaricato. Questo può avvenire in caso di manutenzione del sistema, di sicurezza o di continuità operativa. Se tali operazioni di accesso ai dati o agli strumenti possono avvenire solo con l'utilizzo della password dell'incaricato, è necessario che ogni incaricato, al primo utilizzo della password e successivamente ad ogni cambio, comunichi la sua password in busta chiusa al custode delle password il cui nome sarà comunicato da parte del titolare stesso. Tale comunicazione è necessaria solo nel caso in cui sia necessario conoscere, da parte del titolare e nei casi indicati, la password dell'incaricato. Nel caso in cui il titolare del trattamento possa comunque accedere ai dati senza conoscere tale password (ad esempio tramite la password di amministratore di sistema o resettando la password dell'incaricato o qualora agli stessi dati accedano più persone, evitando quindi la paralisi lavorativa in caso di assenza dell'incaricato) tale procedura non è necessaria.

Protezione dei dati da attacchi di virus o programmi intrusivi
Il titolare del trattamento ha provveduto a installare programmi antivirus e anti programmi pericolosi e ad aggiornarli periodicamente.
E' comunque necessaria anche in questo caso la collaborazione degli incaricati e in particolare, se l'aggiornamento dell'antivirus non è previsto in modalità automatica ma è necessario effettuarlo manualmente a cura di ogni singolo incaricato, tale aggiornamento deve avvenire almeno una volta in settimana.
La maggior parte dei virus vengono diffusi tramite la posta elettronica e Internet; di conseguenza è necessario attenersi alle seguenti ulteriori istruzioni:

- non aprire e- mail che contengano un'estensione doppia;
- prima di aprire una e – mail, in particolare se non richiesta o nel caso in cui si ritenga quantomeno insolita, verificare il mittente ed eventualmente non aprire allegati o collegarsi a siti internet contenuti nel testo della e – mail;
- prima di utilizzare floppy o CD di qualsiasi provenienza, procedere con un controllo da parte dell'antivirus.

Protezione dei dati da distruzione o perdita, anche accidentale
Il titolare del trattamento ha provveduto a installare un sistema di salvataggio centralizzato e automatico dei dati. Il salvataggio viene eseguito a cadenza stabilita e comunque non superiore a sette giorni, da personale appositamente incaricato.
Gli incaricati dovranno però anche in questo caso concorrere e mettere in atto tutte le procedure affinché la misura di sicurezza non risulti inefficace a causa di attività non corrette.
In particolare è necessario che gli incaricati provvedano a salvare tutti i dati sul server evitando di mantenerli in locale sui singoli PC.
E' talora comunque possibile che, a causa del sistema informatico utilizzato o dei programmi installati, i dati siano elaborati in locale sul singolo PC. In tal caso è necessario segnalare la situazione all'amministratore di sistema o al responsabile del trattamento o al titolare il quale provvederà ad attuare le procedure automatiche o manuali al fine di inviare periodicamente i dati sul server in modo tale da procedere al loro salvataggio automatico. Nel caso in cui non sia possibile prevedere l'invio degli archivi sul server, sarà cura dei singoli incaricati provvedere al salvataggio di tali dati. Di regola comunque è opportuno che il salvataggio non avvenga tramite floppy ma tramite masterizzazione su CD. Tale salvataggio dovrà essere eseguito con cadenza almeno settimanale. Naturalmente i supporti sui quali saranno eseguiti i salvataggi dovranno essere conservati in modo appropriato. E' necessario quindi che siano conservati in contenitori chiusi a chiave e protetti (armadi, cassetti,ecc.) o consegnati al soggetto preposto al back up centralizzato.

Protezione dei dati contenuti nei supporti rimovibili
Anche l'utilizzo di supporti rimovibili (floppy, CD, cassette, ecc…) deve essere conforme alle norme di sicurezza previste. In particolare, nel caso tali supporti siano riutilizzati, anche da altri incaricati, e in essi siano contenuti dati sensibili o giudiziari, primo del loro riutilizzo, devono esser cancellate tutte le informazioni contenute, in modo tale da non consentire in alcun modo la conoscenza da parte di terzi di tali dati. Nel caso in cui sia necessario conservare i supporti informatici contenenti dati sensibili o giudiziari, la conservazione deve avvenire in contenitori chiusi a chiave.
Nel caso in cui i supporti informatici siano riutilizzati, anche da altri incaricati, deve essere eseguita la formattazione totale del supporto.
Nel caso in cui, per motivi tecnici, non possa essere eseguita la formattazione, il supporto deve essere distrutto.
Nonostante questa misura minima sia riferita ai dati sensibili o giudiziari, è buona norma applicare questa procedura a tutti i supporti utilizzati, indipendentemente dal tipo di dato registrato. Attenzione al trattamento dei dati dovrà avvenire anche in caso di utilizzo di altri strumenti per i quali sono disposte queste ulteriori istruzioni:

Fax
Verificare la correttezza del numero telefonico relativo al fax dell'utente e porre attenzione alla digitazione del numero telefonico.
Provvedere a stampare sul retro del fax inviato il report di stampa verificando l'esattezza delle pagine inviate e la correttezza dell'invio.
Nel caso in cui siano inviati documenti contenenti dati sensibili o giudiziari provvedere, se possibile, a inviare il documento in due fasi, dividendo il dato identificativo dagli altri dati o, in alternativa, chiamando il destinatario per informarlo dell'arrivo del fax in modo tale che quest'ultimo possa provvedere alla tempestiva raccolta del documento stesso ed eventualmente comunicare al mittente eventuali errori di trasmissione o leggibilità del documento ricevuto.

Fotocopiatrici
Non dimenticare sotto il coperchio della fotocopiatrice il documento da duplicare.
Nel caso in cui il documento contenga dati sensibili o giudiziari provvedere personalmente all'effettuazione della fotocopia e non consegnarlo ad altri soggetti per l'esecuzione del compito.

Scanner
Verificare la correttezza dell'esecuzione, la leggibilità del documento od eventuali errori di acquisizione del testo.

TRATTAMENTI CON STRUMENTI CARTACEI
Protezione dei dati dal rischio di accessi non consentiti agli atti e ai documenti cartacei
Anche gli atti e i documenti cartacei contenenti dati personali devono essere sottoposti a misure di sicurezza. In particolare è necessario che tutti i documenti siano conservati negli apposti armadi, cassettiere, raccoglitori o archivi in genere. E' necessario inoltre che al termine dell'orario lavorativo le scrivanie siano prive di documenti, fascicoli, faldoni contenenti dati personali. Ogni incaricato è responsabile della protezione fisica dei documenti a lui affidati. Particolare attenzione dovrà essere destinata a eventuali stampe dei tabulati prodotti dall'esecuzione di programmi informatici. Le stampe dovranno quindi essere immediatamente raccolte e conservate da parte di chi ha eseguito i comandi di stampa, in particolare se la stampante è condivisa con altri uffici/servizi ed è situata in altri locali. Le stesse procedure dovranno essere attuate per l'utilizzo di fax o fotocopiatrici.
Ulteriore attenzione dovrà essere rivolta alla distruzione dei documenti, ad esempio strappando i documenti prima di cestinarli, o utilizzando i tritadocumenti in particolar modo per atti contenenti dati sensibili o giudiziari o particolarmente riservati.
Ulteriore attenzione dovrà essere rivolta ai documenti contenenti dati sensibili o giudiziari con particolare attenzione alla documentazione sanitaria contenuta nelle schede sanitarie e/o nei piani di assistenza individualizzati quando vengono consultati per l'assistenza giornaliera agli ospiti. A tal fine è necessario che tali documenti, quando sono al di fuori dei loro archivi durante l'utilizzo quotidiano, siano tenuti sotto il controllo e la custodia degli incaricati, mentre al termine dell'impiego quotidiano, devono essere riposti in armadi, cassetti, archivi o contenitori chiusi a chiave. Non devono assolutamente essere lasciati sulle scrivanie o postazioni di lavoro a disposizione di chiunque entri nell'ufficio. In caso di ingresso nel locale di persone estranee è buona norma fare in modo di impedire l'accesso a tali documenti, ad esempio conservandoli temporaneamente in un cassetto o in una teca, sempre comunque sotto il controllo dell'incaricato.
Si ricorda inoltre di provvedere alla separazione dei dati idonei a rivelare stato di salute e vita sessuale da altri dati non necessari alle finalità del trattamento. Ad esempio, i certificati medici possono essere mantenuti nel faldone contenente la documentazione dell'interessato, ma separandoli dagli altri documenti, ad esempio utilizzando una busta chiusa.

UTILIZZO DI ALTRI STRUMENTI
E' possibile che, per il trattamento di dati personali, vengano utilizzati anche altri strumenti quali ad esempio telecamere, macchine fotografiche, cellulari con integrata fotocamere, ecc. Anche per l'utilizzo di tali strumenti è necessario attuare misure di sicurezza. In particolare il rischio più probabile è quello di perdere o dimenticare nei luoghi visitati lo strumento. E' quindi opportuno, se lo strumento è predisposto, inserire un PIN per proteggere i dati inseriti. Tale PIN può essere condiviso con altre persone autorizzate a tali trattamenti o consegnato al custode delle password o al titolare. Una volta effettuate le foto o le riprese, le stesse dovranno essere riversate sul sistema informatico se si utilizzano modelli elettronici e dovranno essere cancellate le immagini dalla memoria dello strumento. Se invece vengono utilizzati modelli non elettronici, le foto sviluppate o le videocassette devono essere conservate con le stesse modalità indicate nella sezione dedicata ai trattamenti con strumenti cartacei.

RESPONSABILITÀ'
Il mancato rispetto o la violazione delle regole contenute nel presente documento potrebbero essere perseguibili con provvedimenti disciplinari. Qualsiasi violazione alla normativa citata da parte degli utenti verrà segnalata alle autorità competenti.

VADEMECUM GARANTE PRIVACY

"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 fini strettamente personali, ad esempio per registrare le lezioni, e sempre nel rispetto delle persone. 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 on line.

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. Lo stesso vale per gli 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 registrare 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.

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 delicati - 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.

NOTA GARANTE PRIVACY 11 SETTEMBRE 2013

Le graduatorie

Il Garante è intervenuto più volte contro illeciti compiuti nella pubblicazione on line di graduatorie di vario tipo, le quali spesso contengono dati personali non pertinenti o eccedenti le finalità istituzionali perseguite. Alcuni Comuni, ad esempio, hanno pubblicato on line le graduatorie di chi ha diritto ad usufruire del servizio di scuolabus includendo tra le varie informazioni liberamente accessibili, non solo i dati identificativi dei bambini, ma anche l'indirizzo di residenza e il luogo preciso dove lo scuolabus li avrebbe fatti salire e scendere. La diffusione di questi dati, oltre a comportare una violazione della normativa, può rendere i minori facile preda di malintenzionati.

Un altro caso frequente riguarda la pubblicazione sui siti Internet degli istituti delle graduatorie di docenti e personale amministrativo tecnico e ausiliario (Ata) per consentire a chi ambisce a incarichi e supplenze di conoscere la propria posizione e punteggio. Tali liste, giustamente accessibili a tutti, non devono però contenere, come in diversi casi segnalati al Garante, i numeri di telefono e gli indirizzi privati dei candidati. Questa illecita diffusione dei contatti personali incrementa, tra l'altro, il rischio di esporre i lavoratori a forme di stalking o a possibili furti di identità.

Il servizio mensa

Il Garante ricorda che è 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. Lo stesso vale per gli studenti che usufruiscono gratuitamente del servizio 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 può 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.

L'iscrizione a scuole e asili

Gli istituti scolastici e gli asili nido, così come i Comuni, devono predisporre con cura i moduli di iscrizione di bambini e studenti, così da non chiedere alle famiglie informazioni personali eccedenti e non rilevanti. Particolare attenzione deve essere posta sull'eventuale raccolta di dati sensibili, come quelli sulle condizioni di salute e sull'appartenenza etnica o religiosa. Il trattamento di questi dati, oltre a dover essere espressamente previsto dalla normativa, richiede infatti speciali cautele e può essere effettuato solo se i dati sensibili sono indispensabili per l'attività istituzionale svolta: non è questo il caso della semplice iscrizione a scuola.