RGPD – Regolamento generale sulla protezione dei dati Regolamento UE/2016/679

Istruzioni ai dipendenti

(Documento approvato dal Consiglio d'Istituto il 17/12/2018)

I dipendenti sono autorizzati al trattamento dei dati personali effettuati svolgendo le proprie mansioni nel rispetto delle istruzioni qui di seguito riportate.

Obblighi di carattere generale

1. Il dipendente può accedere a, utilizzare o condividere i dati personali solo per svolgere le mansioni lavorative assegnategli. In conformità a quanto previsto dal Codice di comportamento dei dipendenti pubblici (d.lgs. 62/13 art. 3 comma 3), il dipendente non usa a fini privati le informazioni di cui dispone per ragioni di ufficio;
2. Il dipendente è consapevole che:
    - il trattamento dei dati personali è consentito solo per lo svolgimento di un compito di interesse pubblico e per l'esercizio di pubblici poteri;
    - I dati particolari possono essere trattati per motivi di interesse pubblico rilevante solo nei casi individuati ad oggi dal Regolamento approvato dal MIUR con il d.m. 305/06. Sono dati particolari i dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
    - la comunicazione di dati personali a terzi e la loro diffusione (ad esempio attraverso la pubblicazione sul sito) sono consentiti solo se previsto dalla legge;
    - i dati particolari non sono di norma pubblicati o diffusi.
3. Il dipendente è consapevole che è possibile raccogliere i dati personali solo previa informativa all'interessato. A tale scopo il dipendente utilizza la modulistica predisposta che riporta l'informativa aggiornata secondo le indicazioni del GDPR;
4. Il dipendente informa, tramite il referente interno della protezione dei dati, il Responsabile della Protezione dei Dati qualora:
    - gli sia richiesto di effettuare trattamenti che ritiene in contrasto con la legge;
    - gli sia richiesto di effettuare trattamenti che non siano previsti dalla legge;
    - ritenga che le misure di sicurezza o organizzative a protezione dei dati non siano attuate o non siano efficaci;
5. Il dipendente si attiene, nel suo operato, alle prescrizioni del Garante per la Protezione dei Dati Personali riportate nel vademecum "La Scuola a Prova di Privacy", allegato alle presenti istruzioni.
6. Il dipendente segnala al Dirigente scolastico o al Responsabile della protezione dei dati eventuali violazioni di dati personali (accessi abusivi, perdita, distruzione, modifiche illecite) non appena ne sia venuto a conoscenza.

Utilizzo delle risorse IT e misure di sicurezza informatiche

7. Le risorse IT assegnate sono utilizzate solo per lo svolgimento delle mansioni lavorative affidate al dipendente;
8. Il dipendente deve proteggere contro l'accesso ingiustificato, la perdita e il furto tutte le risorse IT assegnategli, compresi a titolo non esaustivo computer, dispositivi mobili (smartphone, tablet etc.), unità di archiviazione portatili rilasciati al dipendente (chiavette usb, dischi etc.), applicazioni e database;
9. È severamente vietato utilizzare dispositivi privi di protezione (crittografia, accesso con password…) per conservare o trattare elenchi di dati personali (ad esempio estratti da registri) e documenti contenenti dati di natura particolare (ad esempio dati relativi allo stato di salute o dati giudiziari) o comunque dati personali che è opportuno mantenere riservati (come quelli relativi agli esiti scolastici o a provvedimenti disciplinari);
10. Il trattamento di dati personali può essere svolto solo utilizzando risorse rese disponibili dall'Istituto Scolastico. Il dipendente non può acquisire senza specifica autorizzazione risorse ulteriori (ad esempio servizi cloud);
11. Il dipendente utilizza il software e le applicazioni resi disponibili dall'Istituto Scolastico sistemi on line approntati da enti pubblici per l'erogazione di servizi o l'adempimento di obblighi di legge.
    Il dipendente non acquisisce autonomamente software/applicazioni/servizi on line, anche nel caso in cui siano a titolo gratuito. L'esigenza di nuovi software/applicazioni/servizi on line va segnalato al proprio responsabile;
12. Tutti i computer e i dispositivi mobili assegnati ai dipendenti devono essere protetti tramite credenziali di accesso con funzione automatica di blocco schermo attiva. Il dipendente deve bloccare il proprio dispositivo quando lo lascia incustodito;
13. Il dipendente deve mantenere la riservatezza delle proprie password per l'accesso alle risorse IT e alle varie applicazioni. Le password non possono essere condivise con altri, neppure con i propri colleghi. Il dipendente non può utilizzare password di altri. È ammessa la condivisione della password solo nei casi in cui i sistemi online approntati da enti pubblici ammettano l'accesso solo a un utente generico o consentano un'unica profilazione per l'accesso.
14. Le password devono essere modificate con regolarità, devono essere composte di almeno 8 caratteri, devono contenere almeno maiuscole, minuscole e numeri, possono contenere caratteri speciali (ad esempio @#$%&), e non devono contenere riferimenti facilmente riconducibili al dipendente (tra cui nomi, nomignoli e date personali proprie o di familiari);
15. Il dipendente deve utilizzare una password diversa per ogni sistema o applicazione che la richieda. Non può in alcun modo ricorrere alle stesse password, anche utilizzate in passato, per gli utilizzi personali extralavorativi;
16. Il dipendente deve adottare le dovute misure per prevenire la diffusione di virus, *worm*, messaggi e-mail di *phishing* e software dannosi, evitando di installare software non autorizzati, prestando attenzione ai link presenti nelle mail e evitando di aprire allegati

17. provenienti da mittenti sconosciuti. Tutti i materiali scaricati da internet debbono essere verificati dall'apposito sistema antivirus;
18. L'indirizzo mail assegnato può essere utilizzato solo per lo svolgimento delle proprie mansioni;
19. Qualora la mail debba essere inviata ad una lista di destinatari, il dipendente deve valutare l'opportunità di utilizzare la modalità "copia nascosta" in modo da evitare che gli indirizzi mail contenuti nella lista vengano conosciuti senza che ve ne sia bisogno;
20. Dati personali di natura particolare (ad esempio dati relativi allo stato di salute) possono essere inviati via mail solo se criptati;
21. La casella di posta elettronica non costituisce lo strumento di conservazione e di archiviazione delle comunicazioni dell'Istituto Scolastico. Le mail che abbiano rilievo nell'ambito dei procedimenti amministrativi o per l'erogazione dei servizi sono gestite tramite il protocollo;

Controlli della sicurezza dei sistemi

22. Per garantire la sicurezza dei sistemi, l'utilizzo degli strumenti informatici, in particolare internet, posta elettronica, software e applicazioni, può essere oggetto di verifiche.
23. I controlli vengono effettuati su base anonima o a campione, in conformità con le istruzioni del Garante. Solo nel momento in cui tali verifiche evidenzino la presenza di violazioni, sono effettuati controlli più mirati.

Sicurezza dei dati cartacei

24. I supporti cartacei su cui risiedono dati personali sono gestiti in modo da evitare che vengano persi o siano conosciuti da terzi. A tale scopo:
    - i documenti vanno tenuti sulla scrivania il tempo strettamente necessario ad espletare la pratica e poi vanno riposti negli appositi armadi o scaffali. Nel caso in cui i documenti contengano dati particolari, vanno conservati in armadi chiusi a chiave. Elaborati delle prove scritte e altro materiale relativo alla valutazione degli alunni sono trattati nello stesso modo;
    - nel rapporto con l'utenza, alla scrivania o allo sportello, si fa in modo che le informazioni relative a procedimenti diversi a quelli di interesse non siano visibili o comunque conoscibili;
    - al termine della giornata i documenti non vanno lasciati su tavoli e scrivanie a meno che gli uffici non vengano chiusi a chiave e terzi (imprese di pulizie, pubblico etc.) non vi possano accedere;
    - i documenti possono essere riprodotti solo se necessario allo svolgimento dell'attività e non possono essere lasciati incustoditi presso stampanti o fotocopiatrici condivise o presso aree di pubblico passaggio;
    - i documenti sono condivisi con i propri colleghi solo se necessario;
    - i locali adibiti ad archivio sono normalmente chiusi a chiave. Gli accessi ai locali d'archivio sono consentiti solo dietro autorizzazione del Responsabile della gestione documentale. L'asportazione di documenti dai locali d'archivio è soggetta ad autorizzazione del medesimo responsabile: i dati identificativi dei pezzi prelevati

vengono segnati su un apposito registro, tenuto dal responsabile della gestione documentale

25. Per quanto riguarda la consultazione di documentazione relativa ad alunni con bisogni educativi speciali (BES, compresi alunni con disturbi specifici dell'apprendimento, DSA, e alunni disabili), i docenti della classe in cui è inserito l'alunno hanno accesso ad una copia dei documenti conservata nel faldone del consiglio di classe. La documentazione informatica viene resa disponibile nell'apposita sezione del registro elettronico ed è consultabile da tutti i docenti della classe: i dati rimangono nel registro elettronico e non vengono conservati sui dispositivi dei docenti né trasmessi all'esterno. In ogni caso, i dipendenti si attengono a quanto previsto dalla normativa in merito al rispetto del segreto d'ufficio e professionale secondo quanto previsto dal CCNL e dal Testo Unico sulla Scuola (d.lgs. 297/1994, si veda in particolare art. 494, c. 1, lett. b).