REGOLAMENTO PER L'UTILIZZO DI DISPOSITIVI E DEI DATI RACCOLTI TRAMITE GLI STESSI

PREMESSA

Ai sensi del Regolamento Europeo n. 679/2016 e della normativa in vigore volta alla tutela dei dati personali, questo documento ha lo scopo di fornire alle persone designate e autorizzate al trattamento dei dati personali all'interno dell'Istituzione scolastica nonché agli alunni e alle famiglie, informazioni circa:

- norme comportamentali per un corretto trattamento dei dati personali, delle attrezzature/supporti, delletecnologie informatiche e risorse dell'Istituto utilizzate per trattare dati personali per scopi didattici e professionali;
- istruzioni per la corretta adozione di misure di prevenzione e per la rilevazione e gestione di problematiche connesse ad un uso non consapevole/non adeguato di dati personali.

DOVE TROVARE IL REGOLAMENTO

Il Regolamento sarà reso noto mediante pubblicazione sul sito istituzionale della scuola nella sezione Privacy.

Al nuovo personale sarà comunicato insieme a tutti i documenti da sottoscrivere all'atto della stipula del contratto.

MONITORAGGIO DEL REGOLAMENTO PER L'UTILIZZO DI DISPOSITIVI E DEI DATI RACCOLTI TRAMITE GLI STESSI E SUO AGGIORNAMENTO.

Il Regolamento sarà riesaminato annualmente e/o in caso di modifiche nell'adozione di misure di sicurezza organizzative e tecniche dell'Istituto, nonché in caso di modifiche della normativa.

REGOLAMENTO

1. Gestione accessi e utilizzo attrezzature

- È fatto divieto comunicare a terzi le proprie credenziali/password (as. esempio nessuno deve accederecon un nome utente non suo ai servizi; gli studenti non devono essere in possesso dei dati di login degliinsegnanti e del personale scolastico, etc.)
- Ogni utente deve:
  - spegnere il PC al termine delle ore di lavoro;
  - in caso di assenza momentaneamente dalla propria postazione accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto occorre chiudere la sessione di lavoro sul PC facendo Logout oppure in alternativa occorre avere attivo un salvaschermo (screen-saver) protetto dalle credenziali di autenticazione.

- Quando si esegue la stampa dei documenti occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.
- L'utilizzo dei computer, portatile e attrezzature scolastiche è consentito a fini esclusivamente professionali e didattici.
- Ogni utente deve avere cura delle attrezzature in dotazione segnalando tempestivamente eventuali problemi al Dirigente Scolastico e/o al personale tecnico competente ove presente (es. malfunzionamenti, virus, ecc.) usando i sistemi di difesa e antivirus.
- In caso di un malfunzionamento del PC o in presenza di una violazione dei dati personali (es. diffusione di una foto via internet o sul sito dell'Istituto senza consenso) o qualsiasi altra casistica che può far sospettare un "data breach" (violazione di dati personali) o altra minaccia (es. la presenza di un virus che infetta un pc), l'utente deve:
    - immediatamente sospendere ogni operazione sul PC/dispositivo utilizzato evitando di lavorare con il sistema infetto;
    - contattare immediatamente il docente/responsabile di area/collaboratore tecnico e il Dirigente Scolastico.
- Nessun elemento personale può essere aggiunto al dispositivo in dotazione senza previa autorizzazione da parte della Dirigenza (ad es. scaricare software senza adeguata e valida licenza o altri tipi di risorse da Internet che possono in qualche modo compromettere la rete interna della scuola o che possono bypassare i filtri e i sistemi di sicurezza, non modificare le configurazioni impostate sul proprio PC o rete di istituto, ecc.).
- Si invita il personale scolastico e gli alunni a fare attenzione in caso di apertura di file e allegati "sospetti" e di fare attenzione in caso di collegamenti di memorie esterne (es. controllare sempre la presenza o meno di virus ecc.).
- Il personale scolastico, nell'ambito delle proprie mansioni, ha il compito di salvaguardare il comportamento degli alunni verificando che l'accesso degli studenti avvenga sempre e solamente sotto la propria supervisione e unicamente con gli strumenti messi a disposizione dalla scuola.
- Gli alunni sono tenuti a utilizzare l'attrezzatura messa a disposizione dall'istituzione scolastica (LIM presenti nelle classi, PC portatili, tablet, notebook, ecc.) sempre sotto la supervisione e autorizzazione del docente. Costituiscono eccezione i casi di comprovata necessità (situazioni di disabilità, certificazione DSA) per i quali è possibile l'utilizzo a scuola del PC personale dell'alunno.
- Si invita il personale scolastico e gli alunni ad avere cura di eventuali dispositivi, compresi quelli personali (es. cellulari, palmari, chiavette, dispositivi di archiviazione o altri documenti), evitando di lasciarli incustoditi e a disposizione di estranei (es. al termine dell'orario lavorativo, durante le pause di lavoro, durante riunioni lontane dalla propria postazione, durante intervalli e cambi di ora, ecc.).

2. Gestione documentale

Il personale scolastico autorizzato deve:

- Consegnare alla Segreteria per l'inserimento all'interno dei fascicoli personali ciò che segue:
  1. certificati medici esibiti dagli alunni per qualsiasi motivo;
  2. qualunque altro documento contenente dati personali o sensibili come certificati di malattia, certificati di pronto soccorso e tutta la documentazione inerente allo stato di salute relativo a un interessato;
- Verificare la corretta funzionalità dei meccanismi di chiusura dell'armadietto personale, segnalando tempestivamente al responsabile di sede eventuali anomalie;
- Riporre la documentazione in modo ordinato e negli appositi contenitori (non trasparenti se si tratta didati sensibili), chiudendo a chiave classificatori e armadi dove sono custoditi.

In particolare per i collaboratori scolastici si raccomanda di:

- procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei localisiano state attivate;
- non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte e/o rese anonime;
- non consentire ai non autorizzati di accedere ai documenti dell'ufficio o leggere documenti contenenti dati personali o sensibili.

3. Gestione password e codici di accesso

Le seguenti regole per la gestione delle password si applicano a tutti i servizi informatici, gestionali ed applicativi (compresi quelli web), alle postazioni di lavoro, alla rete wi-fi (ove presenti), al servizio di posta elettronica e a tutte le applicazioni e risorse informatiche (es. registro elettronico) presenti all'interno dell'Istituto che prevedono un sistema di autenticazione per l'accesso.
I sistemi di autenticazione richiedono al soggetto autorizzato di inserire un codice utente (username) ed una parola chiave (password).
L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo dei servizi informatici, e serve a:

- tutelare i soggetti autorizzati al trattamento e l'Istituto da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
- tutelare i soggetti autorizzati al trattamento da false imputazioni, garantendo che nessuno possa operare a loro nome e che, con il loro profilo (ossia con le loro user id e password) solo essi possano svolgere determinate azioni.

Per questi motivi:

- Il personale scolastico e gli alunni non devono comunicare e/o condividere la propria password personale con nessun'altra persona all'interno dell'organizzazione, (colleghi, alunni, personale scolastico, ecc.) e all'esterno (amici, conoscenti, ecc.);
- Nei casi in cui l'utente perda il ruolo, la mansione e le qualità che gli consentono di utilizzare le credenziali per accedere ai vari servizi dell'istituto scolastico, le stesse credenziali devono essere disattivate (es. in caso di cessazione del rapporto di lavoro, trasferimento, licenziamento, sostituzione, ecc.);

- Occorre evitare di memorizzare password e credenziali di accesso su fogli di carta, documenti cartacei e file conservati all'interno della postazione di lavoro (es. non trascrivere la propria password su post it o fogli presso la propria postazione, non memorizzarla in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione internet);
- Gli utenti nella scelta della password devono evitare combinazioni facili da identificare (evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili). Devono scegliere password univoche e originali, che abbiano un senso solo per l'utente che le sceglie, evitando di usare la stessa password per altre utenze.

La password deve essere ragionevolmente complessa e difficile da individuare e/o ricavare.
La password (es. la password d'accesso relative al computer, alla rete, a programmi e software specifici, al salvaschermo) deve essere scelta sulla base dei seguenti criteri:

1. deve essere di lunghezza non inferiore ad 8 caratteri;
2. deve essere obbligatoriamente cambiata al primo utilizzo e successivamente nei casi in cui sia compromessa;
3. deve contenere, ove possibile, almeno 2 caratteri tra numeri, caratteri alfabetici in maiuscolo e minuscolo, e caratteri speciali;
4. non deve essere uguale alle precedenti già utilizzate.

Per la corretta gestione della password occorre:

- modificare le credenziali di autenticazione dopo il primo utilizzo e ogni volta che dovessero sorgere dubbi sulla loro segretezza;
- conservare la password in un luogo sicuro;
- non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, alunni e soprattutto attraverso il telefono (ad. esempio è fatto divieto comunicare agli studenti username e password degli insegnanti e del personale scolastico);
- non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

4. Gestione posta elettronica e-mail

- Gli utenti (es. il personale scolastico) devono utilizzare la propria mail (es. @istruzione.it) per soli fini professionali tenendola separata dalla e-mail privata.
- Nel caso in cui qualcuno appartenente alla comunità scolastica (alunno, docente, personale) riceva e- mail da considerare particolarmente preoccupanti (es. mail con contenuti pedo pornografici) dovrà mettersi in contatto con il personale scolastico e/o, a seconda della gravità, direttamente con gli organi di Polizia Postale.
- Il trasferimento di dati sensibili, ove consentito, per il personale docente, è possibile tramite invio di file PDF con codice per l'apertura del file stesso.
- Ogni utente che utilizza la posta elettronica dovrà prestare massima attenzione a rispondere ad e-mail sospette e/o a cliccare sui link durante la navigazione web (o su link presenti all'interno delle mail) al fine di contrastare possibili frodi informatiche (come il phishing, lo spear phishing, il furto d'identità,ecc.).

- Il personale scolastico potrà mettersi in comunicazione con alunni e genitori (e viceversa) solo per ragioni e fini chiaramente istituzionali e professionali utilizzando gli appositi canali ufficiali.
- Per un corretto utilizzo della posta elettronica l'utente è invitato a:
  1. non aprire documenti di cui non sia certa la provenienza;
  2. controllare accuratamente l'indirizzo del destinatario prima di inviare dati personali.

5. Gestione back up e Cloud computing

- Gli utenti sono invitati a non condividere e/o memorizzare dati personali relativi alla propria sfera privata (foto della propria famiglia e/o amici, dei luoghi di abitazione, amici, ecc.) all'interno dello spazio online e/o supporti di archiviazione appartenenti all'istituto scolastico.
- Il personale scolastico è invitato a non condividere e/o memorizzare dati personali relativi alla propria attività istituzionale (es. dati personali e sensibili relativi agli studenti) su servizi di hosting pubblici (es. Google Drive, Dropbox, ecc.) salvo specifiche e chiare autorizzazioni da parte del Dirigente Scolastico.
- È fatto divieto memorizzare dati sensibili su supporti non protetti con tecniche di cifratura (es. usb, dispositivi di archiviazione mobili, ecc.).

6. Social network e navigazione internet

Il personale scolastico (es. insegnanti, esperti, educatori, collaboratori, ecc.):

- Non dovrà intraprendere attività online (es. attraverso l'utilizzo di social, chat, forum, blog, ecc.) che possa compromettere la propria reputazione, le proprie responsabilità professionali e che possa portare discredito all'Istituto scolastico con le sue opinioni personali. Si raccomanda quindi di:
- evitare di scaricare/inviare materiali che possano essere considerati offensivi;
- assicurarsi che tutti gli spazi social e di condivisione utilizzati come privato cittadino siano nettamente distinti e non possano essere confusi con il proprio ruolo professionale (es. non fare riferimento a studenti/alunni, genitori/tutori o personale scolastico, non entrare in discussioni online su questioni personali relative agli stessi membri della comunità scolastica, non attribuire opinioni personali alla scuola o alla sua dirigenza o alle autorità locali, ecc.);
- utilizzare i sistemi dedicati, ufficiali e istituzionali della scuola per l'effettuazione di eventuali comunicazioni nei confronti di studenti e famiglie (es. tramite utilizzo di apposita mail istituzionale);
- prestare attenzione a eventuali diritti d'autore (royalty) prima di pubblicare o distribuire qualsiasi opera intellettuale tra cui immagini, musica, video, registrazioni vocali;
- non aprire, scaricare, installare o utilizzare files/applicazioni/software sospetti e/o di dubbia provenienza (si raccomanda l'utilizzo del protocollo HTTPS);
- prestare massima attenzione in caso di comportamenti anomali su social network (es. Facebook, Twitter, Instagram, ecc.) su sistemi di messaggistica istantanea, accertandosi, per quanto possibile, che gli studenti, in caso di utilizzo di smartphone o altra apparecchiatura elettronica all'interno dell'istituto scolastico, non diffondano immagini e dati personali senza previo consenso dell'interessato (proprietario del dato);

- mantenere la massima riservatezza riguardo al segreto d'ufficio e professionale (es. riguardo a dati eventualmente contenuti nei temi degli alunni specialmente se riguardano argomenti delicati e strettamente relativi alla sfera privata, riguardo alle condizioni di salute di colleghi e studenti, ecc.).

Le famiglie e gli alunni:

- Sono resi consapevoli che l'Istituto Scolastico prenderà precauzioni ragionevoli per mettere in sicurezza i propri utenti evitando che gli studenti accedano a materiali inappropriati;
- Sono invitati a sostenere e collaborare con l'Istituto Scolastico promuovendo l'uso sicuro di Internet e delle tecnologie digitali a casa, informando la scuola in caso di preoccupazioni al riguardo;
- Nel caso in cui gli stessi alunni vedano o sentano qualcosa che possa turbare la propria privacy (ad es. la ricezione di un messaggio che possa farli sentire a disagio) sono invitati a parlarne con un adulto di fiducia (genitori o nel caso i propri docenti).

7. Gestione strumentazione personale: uso dei cellulari e dispositivi mobili

Regole generali

- Il personale, gli esperti di progetto, gli studenti, i genitori e/o i visitatori che portano all'interno dell'Istituto *device* di loro proprietà, sono responsabili del proprio dispositivo e lo portano nell'Istituto a proprio rischio. Si puntualizza che, se il device viene smarrito, si rompe, viene danneggiato, vengono persi dei dati ecc., la scuola non deve essere considerata responsabile della sicurezza di tali dispositivi/dati né deve farsi carico di eventuali risarcimenti, a meno che l'Istituto non si assuma la custodia del *device* stesso.
- L'istituzione scolastica si riserva il diritto di reperire contenuti presenti all'interno di qualsiasi dispositivo presente nei locali della scuola, qualora vi sia il ragionevole sospetto che esso possa contenere materiale illegale o indesiderabile (es. riguardante la pornografia, la violenza o il bullismo, registrazioni di qualsiasi genere vietate, ecc…).
- L'utilizzo del cellulare, di apparecchi per la registrazione di suoni e immagini è in genere consentito, ma esclusivamente per fini didattici (recite, video lezioni, attività progettuali, ecc.), nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte, in particolare della loro immagine e dignità.
- Si ricorda che prima di ogni utilizzo o eventuale diffusione di contenuti, anche su Internet, è necessario informare adeguatamente le persone coinvolte nella registrazione (professori, studenti, ecc…) e ottenere il loro esplicito consenso.
- Deve essere sempre garantito il diritto degli studenti con diagnosi DSA (disturbi specifici dell'apprendimento) o altre specifiche patologie all'utilizzo di tutti gli strumenti compensativi di volta in volta previsti nei piani didattici personalizzati che li riguardano (ad. esempio il registratore).
- Non violano la privacy le riprese video e le fotografie raccolte durante le recite, le uscite didattiche, i viaggi di istruzione 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.

Per gli studenti e le famiglie

Caso 1. Utilizzo del telefono cellulare/tablet/altri dispositivi mobili personali ad uso assimilabile al privato per chiamate, sms, messaggistica in genere, ecc.

- Durante l'orario delle lezioni (es. durante gli esami, verifiche, prove nazionali) l'uso di device personali non è consentito (es. per ricevere/effettuare chiamate, navigazione su internet, SMS o altro tipo di messaggistica, gioco, ecc.);
- Gli alunni sono tenuti a fare buon uso dei propri telefoni/device;
- Per quanto riguarda uscite, visite guidate e viaggi di istruzione, l'uso può essere consentito, se autorizzato dal docente, al di fuori dei momenti dedicati alle attività strettamente legate all'aspetto didattico dell'uscita;
- La comunicazione con le famiglie, per qualsiasi urgenza, è sempre garantita attraverso il telefono della scuola (i docenti possono però consentire l'uso del cellulare, in caso di particolari situazioni non facilmente risolvibili in altro modo, ad es. in casi di particolare emergenza e grave pericolo per le persone);
- Le famiglie degli studenti sono invitate a collaborare strettamente con l'Istituzione scolastica nello spirito della corresponsabilità educativa (es. evitando di inviare messaggi o effettuare chiamate ai telefoni dei propri figli durante l'orario scolastico o visite di istruzione).

Caso 2. Utilizzo delle funzioni tipiche degli smartphone, tablet, notebook e altri dispositivi mobili (foto, video, scrittura collaborativa e condivisione di documenti, ecc.), per le attività didattiche a scopi professionali.

- In questo caso l'uso di smartphone, tablet e altri dispositivi mobili personali, è consentito. I dispositivi mobili personali verranno utilizzati unicamente durante le lezioni solo come parte di un'attività curriculare e secondo le modalità prescritte dall'insegnante e con esclusiva finalità didattica;
- Si ricorda che la diffusione di filmati e foto che ledono la riservatezza e la dignità di sé e di altre persone (es. eventuali riprese audio/video o fotografiche effettuate all'interno degli ambienti scolastici e successivamente diffuse con l'intento di ridicolizzare compagni o insegnanti o addirittura allo scopo di intraprendere azioni denigratorie, intimidatorie, vessatorie) può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati. Anche in questo caso si richiede grande sintonia e collaborazione tra scuola e famiglia, in modo da favorire lo sviluppo della necessaria consapevolezza e maturità circa l'utilizzo degli strumenti ai quali gli studenti abbiano accesso.

Per il personale scolastico (es. docenti, educatori, esperti di progetto)

- L'uso di smartphone, tablet e altri dispositivi mobili è consentito con esclusiva finalità professionale e solo in caso di particolari necessità (es. evacuazione dell'Istituto, emergenze);
- L'uso del cellulare/tablet non è consentito, salvo autorizzazione della Dirigenza, per ricevere/effettuare chiamate personali, SMS o altro tipo di messaggistica durante l'orario di lavoro.

8. Gestione violazioni/infrazioni

Qualsiasi ipotesi di violazione dei dati personali va segnalata immediatamente al Dirigente Scolastico.
Il personale, genitori e gli stessi alunni sono invitati a collaborare responsabilmente per la sicurezza a scuola.
Al personale, agli studenti e agli altri componenti della comunità scolastica sono date informazioni sulle infrazioni previste e le eventuali sanzioni (Regolamento di disciplina).
Le sanzioni riferite soprattutto agli alunni avranno come carattere preferenziale quello educativo/riabilitativo e in ogni caso verrà coinvolta la componente genitori, in qualità di primi educatori.

9. Note conclusive

In conclusione, si invitano tutti i membri della comunità scolastica (personale docente, collaboratori, famiglie e alunni, ecc.) a collaborare strettamente con l'Istituzione scolastica nello spirito della corresponsabilità educativa e della salvaguardia della protezione dei dati personali.

La Dirigente Scolastica
Dott.ssa Nadia Tantardini
Documento firmato digitalmente ai sensi
del CAD e normativa connessa