APIS004007 - REGISTRO PROTOCOLLO - 0011577 - 08/10/2021 - A14 - Privacy - I

ISTITUTO DI ISTRUZIONE SUPERIORE - OMNICOMPRENSIVO DI AMANDOLA
Via C. Baiocchi, 1 - 63857 AMANDOLA FM - Tel. 0736847516 - Fax 0736847408 – E-mail: apis004007@istruzione.it
Codice Meccanografico: APIS004007 - Codice Fiscale: 80007950449 – PEC: apis004007@pec.istruzione.it
Sito Web: www.iis-amandola.edu.it con sezioni associate

LINEE GUIDA OPERATIVE
PER
ASSISTENTI AMMINISTRATIVI AREA DIDATTICA

Richiamate le prescrizioni previste nell'atto di nomina ad incaricato al trattamento dei dati, così come quelle stabilite nelle linee guida generali afferenti il personale scolastico, vengono di seguito indicate le misure operative da adottare per garantire la sicurezza dei dati personali da parte degli incaricati al trattamento facenti parte dell'unità organizzativa "Assistenti amministrativi: Area Didattica".

Le misure operative vengono suddivise a seconda che trattasi di:
1. Trattamenti manuali e cartacei.
2. Trattamenti elettronici o digitali
3. Affissione documenti contenuti dati o Pubblicazione di Dati Online.

- 1 -
TRATTAMENTI MANUALI E CARTACEI

Il trattamento manuale seppur oramai quasi in disuso può comunque riguardare (per esigenze organizzative particolari o comunque in via generale) i seguenti documenti:
- Certificati medici esibiti dagli studenti;
- Certificati contenenti dati reddituali e/o giudiziari;
- Raccolta delle domande di iscrizione presentate online o in modalità cartacea e gestione delle iscrizioni per l'accoglimento della domanda;
- Gestione del percorso scolastico, formativo e amministrativo dell'alunno e alimentazione e aggiornamento dell'Anagrafe Nazionale degli Studenti
- Qualunque altro documento che dovesse comunque essere esibito direttamente dall'interessato e che contenga dati personali o particolari/sensibili relativi a Studenti, Famiglie

Con riferimento ai trattamenti manuali l'incaricato dovrà attenersi alle seguenti prescrizioni operative:
Documenti in ingresso.
Per "documenti in ingresso", si intendono i documenti contenenti dati personali acquisiti dalla scuola ai fini di un loro impiego in trattamento. Relativamente al trattamento dei documenti in ingresso, è necessario adottare le cautele seguenti:
- I documenti in ingresso devono essere utilizzati soltanto da chi sia Incaricato al trattamento dei dati che contengono e, nel caso in cui si venga in contatto con dati non di propria pertinenza, provvedere alla immediata trasmissione al soggetto incaricato, notiziando della circostanza il responsabile

Firmato digitalmente da RITA DI PERSIO

- L'Incaricato deve altresì verificare:
  - la provenienza dei documenti;
  - che tali documenti siano effettivamente necessari al trattamento in questione;
  - la tipologia dei dati contenuti (comuni, sensibili, giudiziari o altri dati particolari), al fine di individuare le modalità legittime ed idonee per il trattamento e le misure di sicurezza da attuare;
  - l'osservanza del principio di pertinenza e non eccedenza rispetto o alle finalità del trattamento, la completezza, la correttezza e l'aggiornamento dei dati
  - che al soggetto che fornisce il dato sia stata preventivamente fornita l'informativa o, in caso contrario, provvedervi nell'immediatezza

Gestione ed uso dei Documenti

L'incaricato opererà il trattamento dovuto secondo le seguenti indicazioni:

- evitare in qualsiasi modo di lasciare incustoditi i documenti raccolti;
- divieto di affissione, salvo questa sia dovuta per norme di legge o regolamentari, in qualsiasi luogo di documentazione inerente le posizioni dei "dipendenti scolastici";
- divieto di svolgere attività di ricerca con la raccolta di informazioni personali tramite questionari da sottoporre ai dipendenti scolastici;
- in nessun caso è concesso l'accesso a documentazione contenente dati personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- la documentazione contenente dati personali che, per ragioni di praticità operativa, risiede sulle scrivanie delle persone autorizzate, deve comunque essere rimossa al termine dell'orario di lavoro;
- la documentazione contenente dati particolari (sensibili, giudiziari, afferenti lo stato di salute, ecc.) deve essere usata per il tempo strettamente necessario, per poi essere prontamente archiviata, senza restare sulla scrivania del personale, in particolar modo incustodita.
- i documenti contenenti dati personali non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
- è severamente vietato utilizzare documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti;
- il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
- registrare, ove dovuto, i dati cartacei pervenuti sugli applicativi informatici avendo cura di inserire solo le informazioni minime indispensabili e quelle di default indicate nel programma;

Archiviazione/Custodia dei Documenti.

I Documenti Contenenti dati personali dovranno essere custoditi/archiviati – conclusasi l'operazione del caso specifico - secondo le seguenti modalità:

- Negli archivi in uso alle segreteria di riferimento (in armadietti dotati di serrature), mediante suddivisione in fascicoli riferiti al singolo soggetto e, al suo interno, sotto fascicolo separato per i dati sensibili a c.d. bassa pericolosità che, infatti, si situano in una sostanziale zona grigia (es. certificati medici generici privi di diagnosi);
- In archivio separato, ad alta sicurezza (le cui chiavi saranno in possesso del solo titolare del trattamento), per tutti quei documenti contenenti dati particolari ad alto livello di delicatezza (l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici e i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona), che dovranno, tra l'altro, essere riposti in buste di carta chiusa, su cui verrà indicato il nome dell'interessato ed il tipo di documento.

TRATTAMENTI ELETTRONICI E DIGITALI

A. UTILIZZO DI DISPOSITIVI INFORMATICI IN USO ALL'INTERNO DELLE AULE ADIBITE AD USO SEGRETERIA:

La segreteria amministrativa dell'Istituto Omnicomprensivo ha a disposizione diversi computer per i servizi di accesso ai software utilizzati per la gestione delle attività di sua competenza.

In merito ai computer in uso all'interno della segreteria si rappresentano i seguenti rischi:
- Rischio interno relativo all'utilizzo della rete da parte di personale non autorizzato ad accedere ai dati.;
- Rischio interno dovuto a intrusioni da parte di studenti e/o terze persone;
- Rischio esterno relativo all'accesso ai dati da parte di persone estranee attraverso eventuali punti di ingresso/uscita verso internet;
- Rischio esterno dovuto ad intrusioni nel sistema da parte di hacker/cracker;
- Rischio interno/esterno di scaricamento virus e/o trojan per mezzo di posta elettronica e/o operazioni di download eseguite tramite il browser.

Per ovviare a tali rischi si dà disposizione a che:
1) Gli strumenti informatici in dotazione all'interno della segreteria vengano utilizzati secondo la configurazione standard dei dispositivi elettronici, e dunque non vanno in alcun modo modificate le misure di sicurezza già predisposte o i settaggi configurati di default;
2) In caso di avaria o di mal funzionamento del computer contattare gli assistenti tecnici per la riconfigurazione del sistema standard;
3) Le credenziali di autenticazione (per accedere agli strumenti informatici di ogni aula) devono essere custodite con cura e diligenza; non possono essere messe a disposizione né rivelate a terzi; non possono essere lasciate incustodite, né in libera visione. In caso di smarrimento o furto bisogna dare immediata comunicazione al d.p.o. dell'istituto;
4) Si svuoti il cestino del desktop ogni volta che si elimina un documento o si termina una sessione di lavoro;
5) Si eviti di abbandonare la propria postazione di lavoro senza aver effettuato la disconnessione utente o aver inserito uno screensaver con password;
6) In caso di necessità d'utilizzo di dispositivi mobili (usb – meg- etc..) è necessario non avviare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi rimovibili;
7) Gli strumenti informatici vengano inibiti all'uso diretto ed autonomo da parte di soggetti terzi (studenti, docenti, collaboratori tecnici, etc..).

B. POSTA ELETTRONICA DIGITALE.

All'atto di immissione in servizio al personale della segreteria amministrativa viene attribuita una email personale con dominio "@iis-amandola.it". Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi, interni o esterni, per le finalità dell'Istituto Scolastico. Al fine di non compromettere la sicurezza dell'Istituto bisogna adottare le seguenti norme comportamentali:
- All'atto di ricezione dello user e della password di attribuzione della mail è necessario procedere alla modifica della password;
- La pass deve essere modificata ogni 6 mesi;

- Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
- La casella di posta elettronica deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati;
- È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list;
- Verificare sempre che l'indirizzo del destinatario sia stato correttamente digitato;
- L'oggetto del messaggio deve contenere sempre e solo indicazioni neutre senza alcun riferimento a stati, fatti o qualità idonei a rilevare dati di natura sensibile;
- In caso di dati sensibili, nel corpo del messaggio deve essere presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.

C. IL SOFTWARE NUVOLA

Per consentire la dematerializzazione e lo snellimento delle procedure, nonché per garantire e promuovere l'accesso all'informazione da parte di studenti e famiglie e dipendenti, questo Istituto ha adottato, il software "NUVOLA" a cui si può accedere tramite il seguente link: https://nuvola.madisoft.it/login

Tutte le operazioni relative all'uso dello stesso sono improntate alla tutela della privacy ed ogni tipologia di utente ha accesso - ed è autorizzato a trattare - solo informazioni strettamente pertinenti al proprio ruolo.
Per quanto di vostro interesse, il software NUVOLA gestisce anche dati afferenti gli studenti, le famiglie o esercenti la responsabilità genitoriale, così come i profili prettamente didattici dei docenti dati che sono soggetti alle norme che tutelano la privacy.
La titolarità del trattamento dei dati personali è esercitata dal Dirigente Scolastico mentre è nominato responsabile esterno del Trattamento dei dati la "Madisoft SpA".
Tutti gli amministrativi inquadrati nell'Area "Didattica" utilizzano il software Nuvola per svolgere le attività inerenti esclusivamente alla posizione di studenti e famiglie.
Per la gestione delle attività gli incaricati potranno accedere all'Area **"Alunni e Didattica"** del software Nuvola, o, in caso di assenza degli operatori addetti all'unità organizzativa "Assistenti amministrativi – Area Protocollo" alla sezione "Amministrazione Digitale"
Le credenziali di accesso al registro verranno comunicate via e-mail dall'Istituzione scolastica all'indirizzo di posta elettronica istituzionale attribuita all'amministrativo. La password assegnata inizialmente all'amministrativo deve essere cambiata al primo utilizzo e deve essere poi modificata periodicamente ogni 6 mesi. E' vietato cedere, anche solo temporaneamente, il proprio codice utente e la propria password. L'utente intestatario verrà considerato responsabile di qualunque atto illecito perpetrato con quell'account.
Le credenziali di accesso di ogni incaricato rimangono attive fino alla permanenza dell'incaricato in servizio nell'istituto.
Esse non devono essere memorizzate in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione Internet o in computer di uso comune. Ogni incaricato, per accedere al registro elettronico, deve inserire le proprie credenziali: username e password; alla fine del suo utilizzo deve assicurarsi di aver chiuso il proprio account. L'accesso al software Nuvola e all'area Docenti potrà essere effettuato utilizzando i computer di cui la scuola dispone oppure, nel caso di cattivo funzionamento dei primi, utilizzando i dispositivi personali, collegati alla rete WIFI dell'Istituto.
Si raccomanda, inoltre, agli incaricati di non allontanarsi mai e per nessuna ragione dalla postazione di lavoro lasciando aperto il software applicativo.

D. LA PIATTAFORMA SIDI

Il SIDI (Sistema Informativo Dell'Istruzione) è un'area riservata in cui sono disponibili le applicazioni (e relative comunicazioni) per le segreterie scolastiche e gli uffici dell'Amministrazione centrale e periferica che hanno il compito di acquisire, verificare e gestire i dati che il sistema informativo raccoglie ed elabora.

Di seguito alcuni esempi di dati gestiti:

- Rete scolastica (in termini di istituzioni scolastiche statali e non statali)
- Dati di funzionamento e organizzativi dell'offerta formativa didattica (indirizzi di studio, Alunni, Organici, Personale docente e non docente)
- Dati finanziari e contabili
- Rilevazioni dati

Per le procedure di abilitazione al SIDI potete consultare la guida presente nel sito https://www.miur.gov.it/-/sidi

L'accesso all'area riservata del portale SIDI potrà essere effettuata tramite il seguente link: "https://www.miur.gov.it/web/guest/accesso"

All'interno della piattaforma SIDI sarà consentito l'accesso nell'ambito delle funzioni attribuite all'interno dell'organizzazione dell'istituto Scolastico e, nello specifico, in relazione alla presente unità organizzativa alle seguenti aree:

- Gestione anno scolastico
- Rilevazioni

Titolare del trattamento dei dati è il Ministero dell'Istruzione, dell'Università e della Ricerca, viale Trastevere 76/A, 00153, Roma, al quale ci si potrà rivolgere per esercitare i diritti di cui all'articolo 7 del D.Lgs. cit e/o per conoscere l'elenco aggiornato di tutti i Responsabili del trattamento dei dati.

E. UTILIZZO DI DISPOSITIVI HARDWARE PERSONALI

In caso di smartworking o di esigenze particolari gli incaricati sono autorizzati all'utilizzo di computer e hardware personali. In tal caso compete all'incaricato accertare:

- Sicurezza degli end point (pc, tablet, notebook, smartphone), ovvero di utilizzo di dispositivi personali per scopi aziendali: aggiornare sempre il sistema operativo e l'antivirus (attenzione a quelli gratuiti!);
- Utilizzo di connessioni sicure: le VPN creano un canale sicuro di collegamento tra il dispositivo di casa e la rete scolastica, instaurando un sistema di controllo con duplice inserimento di credenziali (per rendere il tutto più sicuro è buona norma criptare anche il flusso di dati, così da renderlo non intelligibile a chi riuscire a "bucare" il canale);
- Corretto utilizzo dei device: non devono essere usati per scopi personali, ove forniti dall'Istituto Scolastico, (attenzione ai figli minori, alle piattaforme di gioco online, ecc.: gli utenti che prestano poca attenzione alla sicurezza aumento esponenzialmente il rischio!)
- Controllo sulle reti domestiche (smart tv, telefono, computer): se una minaccia si nasconde nella rete domestica può girare liberamente e penetrare anche in quella scolastica (island hopping);
- Corretto utilizzo della mail istituzionale: uso ben distinto e separato rispetto a quello della mail personale.

AFFISSIONE DOCUMENTI CONTENUTI DATI, COMUNICAZIONI E PUBBLICAZIONE DI DATI ONLINE

In merito al punto in oggetto si ricorda che le Istituzioni Scolastiche non possono pubblicare, per finalità di trasparenza, qualunque dato o informazione personale, ma, per poter procedere lecitamente alla pubblicazione degli stessi, anche mediante internet, sono tenute a individuare un **preciso riferimento legislativo o regolamentare**, che legittimi la diffusione del dato personale.
L'Istituzione Scolastica, dunque, laddove individui un obbligo normativo che impone la pubblicazione di un atto o di un documento sul proprio sito web istituzionale, deve limitarsi a includere negli atti da pubblicare solo quei dati personali espressamente indicati dalla normativa di riferimento o comunque realmente necessari e proporzionati alla finalità di trasparenza perseguita nel caso concreto, valutando anche la possibilità di ricorrere all'oscuramento di determinate informazioni.
Inoltre, le "particolari categorie di dati" (l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici e i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) possono essere trattate solo se indispensabili, ovvero se la finalità di trasparenza non può essere conseguita con dati anonimi o personali di natura diversa. A tal proposito, il Garante della privacy ha avuto occasione di precisare che, per anonimizzare un documento, non è sufficiente sostituire il nome e cognome con le iniziali dell'interessato, ma occorre oscurare del tutto il nominativo e le altre informazioni riferite allo stesso, che ne possono consentire l'identificazione anche a posteriori.
Per quanto di competenza ed a titolo esemplificativo si segnala come il Garante della Privacy, in esplicita FAQ, ha precisato che nelle comunicazioni scuola-famiglia non possono essere inseriti dati personali degli alunni: **nelle circolari, nelle delibere o in altre comunicazioni non rivolte a specifici destinatari non possono essere inseriti dati personali che rendano identificabili gli alunni (ad esempio, quelli coinvolti in casi di bullismo o quelli cui siano state comminate sanzioni disciplinari o interessati da altre vicende delicate).**

La Dirigente Scolastica
Prof.ssa Rita di Persio

Firmato digitalmente da RITA DI PERSIO