Ministero dell'Istruzione, dell'Università e della Ricerca
UFFICIO SCOLASTICO REGIONALE PER L'ABRUZZO
Direzione Generale -L'Aquila-

IL DIRETTORE GENERALE

VISTO l'art. 26, comma 8, della legge 23.12.1998, n.448, che prevede l'assegnazione di dirigenti scolastici e docenti per lo svolgimento di compiti connessi con l'attuazione dell'autonomia scolastica;

VISTA la Circolare ministeriale n. 11233 del 10 aprile 2019 che definisce le procedure per l'individuazione del personale scolastico da destinare ai compiti e ai progetti di cui all'art. 26, comma 8, legge 448/98;

CONSIDERATO che la predetta nota, ai fini della selezione del personale da assegnare a supporto dell'autonomia scolastica (art. 26 legge 448/98 – comma 8 – primo periodo) richiama le modalità consuete di cui alla C.M. n. 14 del 3 luglio 2015;

VISTA la C.M. n. 14/2015 ed in particolare il punto 4 che prevede la costituzione di un'apposita Commissione che dovrà esaminare i candidati e redigere una graduatoria di merito, sulla base dei titoli presentati e di un colloquio finalizzato all'accertamento delle capacità relazionali e delle competenze coerenti con le problematiche delle aree di utilizzazione;

VISTO il regolamento UE 2016/679 (GDPR) e il D.Lgs 196/03 in materia di protezione dei dati personali;

ACQUISITA la disponibilità dei dirigenti sotto citati;

D I S P O N E

ART. 1) E' costituita, ai sensi della C.M. n. 14 del 3 luglio 2015 e ai fini degli adempimenti di cui in premessa, la seguente Commissione:

Presidente dott. Massimiliano NARDOCCI – Dirigente U.S.R. Abruzzo - L'Aquila;

Componenti dott.ssa Rita Anna SEBASTIANI -Dirigente U.S.R. Abruzzo in quiescenza-
Prof. Carlo DI MICHELE Dirigente Scolastico -I.C. S. Vito Chietino (CH)-

Le funzioni di **segretario** saranno svolte dal sig. Vinicio BUCCI -Area II/F6- dell'U.S.R. Abruzzo.

Per l'espletamento di tale incarico ai componenti della Commissione non compete alcun compenso ad eccezione delle indennità di missione, qualora spettanti.
La Commissione è autorizzata a svolgere i propri lavori presso questa sede dell'U.S.R. Abruzzo.

ART. 2) I componenti la Commissione tratteranno i dati richiesti ai candidati ai sensi e con le garanzie di cui agli articoli 6 e 13 del Regolamento UE 2016/679 (GDPR) e dell'art. 7 del D.Lgv 196/03 (codice in materia di protezione dei dati personali). A tal fine:
I componenti della Commissione di cui all'art. 1, incluso il segretario, sono autorizzati al trattamento di tutti i dati personali nonché di tutte le operazioni/tipologie di trattamento, secondo quanto riportato nell'**allegato A-**
I componenti della Commissione di cui all'art. 1, incluso il segretario, sono tenuti a limitare il trattamento dei dati a quanto necessario ed indispensabile all'adempimento delle funzioni e delle mansioni assegnate, osservando inderogabilmente le norme di legge, i regolamenti interni, le linee guida di riferimento, le circolari, gli ordini di servizio, le istruzioni comunque impartite dal Titolare del Trattamento e/o dai suoi Designati nonché quanto riportato nell'**allegato B**.

Il Direttore Generale
Antonella Tozza
Documento firmato digitalmente ai sensi del
Codice dell'Amministrazione Digitale e normativa connessa

Allegato A - Ambito del trattamento consentito e finalità

Mansioni assegnate al soggetto Autorizzato che prevedono trattamento di dati personali	Ambito del trattamento consentito	Finalità
1) Commissione esaminatrice, incluso il segretario.	**a**) valutazione delle istanze di partecipazione alla procedura di selezione degli aspiranti all'assegnazione presso l'USR Abruzzo per lo svolgimento di compiti connessi all'autonomia scolastica anche con attività di verbalizzazione. **b**) Predisposizione della graduatoria. **c**) Reclami.	Individuazione candidati per l'utilizzazione nel triennio 2019/2022 presso l'USR per l'Abruzzo.

Allegato B - Istruzioni

1. Tipologie di dati trattati

(Indicare le tipologie di dati personali trattati in linea con quanto indicato nel Registro delle attività di trattamento)

a) Dati personali identificativi riferiti a (ex articolo 5 GDPR):

- Aspiranti all'assegnazione presso l'USR per l'Abruzzo sede di L'Aquila per lo svolgimento di compiti connessi all'autonomia scolastica, a seguito di istanza di parte, come da modello di domanda utilizzato;
- personale della scuola (dirigenti scolastici e docenti);

b) Dati personali di natura particolare (ex art. 9 GDPR) riferiti a:

- certificazioni legge 104/92, inserimenti legge 68 per la valutazione (eventuale) dei titoli di preferenza/precedenza etc come da istanza di aggiornamento/nuovo inserimento presentata dal soggetto istante

c) Dati personali giudiziari (ex articolo 10 GDPR) riferiti a soggetti coinvolti nei procedimenti amministrativi o giudiziari di competenza:

- Dichiarazioni rese in seno alla istanza di partecipazione con riferimento al casellario giudiziario e agli eventuali carichi pendenti.

2. Principi

Il soggetto Autorizzato al trattamento dei dati personali deve:

- assicurare la riservatezza, nonché la protezione dei dati personali dei quali venga a conoscenza durante l'esecuzione delle attività svolte;
- utilizzare i dati personali solo per le finalità connesse allo svolgimento delle attività e per le finalità di cui all'allegato A, con divieto di qualsiasi altra diversa utilizzazione;
- porre in essere tutte le azioni idonee a garantire il rispetto delle vigenti disposizioni in materia di protezione dei dati personali, segnalando tempestivamente al soggetto Designato ogni eventuale problema applicativo;
- garantire il rispetto della normativa nelle attività di consultazione e gestione della documentazione contenente dati personali, con riguardo anche alla custodia ed archiviazione della stessa;
- salvaguardare la conformità delle riproduzioni dei documenti agli originali ed evitare ogni azione diretta a manipolare, dissimulare o deformare fatti, testimonianze, documenti e dati;
- controllare e custodire fino alla restituzione gli atti e i documenti contenenti dati personali affidatigli per lo svolgimento dei propri compiti in maniera che ad essi non accedano persone prive di autorizzazione, restituendoli al termine delle operazioni affidate;
- rispettare le misure di sicurezza volte a prevenire l'eventuale distruzione, dispersione o accesso non autorizzato ai documenti, adottando, in presenza di specifici rischi, particolari cautele quali la consultazione in copia di alcuni documenti e la conservazione degli originali in cassaforte o armadi blindati, ove presenti;
- non fare alcun uso improprio e mantenere riservate le notizie e le informazioni concernenti i dati personali non resi pubblici, appresi nell'esercizio delle proprie attività, osservando tali doveri di riserbo anche dopo la cessazione dell'attività lavorativa.

I dati personali devono essere trattati nel rispetto dei seguenti principi:

- **liceità:** ogni trattamento deve essere conforme alle disposizioni in materia di protezione dei dati personali e, in particolare, nella misura in cui ricorra almeno una delle condizioni di cui all'art. 6, par. 1, del Regolamento;

- **correttezza e trasparenza:** il trattamento deve essere esplicitamente chiarito agli interessati, fornendo loro le informazioni necessarie a far comprendere in modo adeguato non solo le modalità del trattamento, ma anche le eventuali conseguenze;
- **sicurezza e riservatezza:** devono essere realizzate misure tecniche e organizzative di sicurezza appropriate ai rischi presentati dal trattamento, secondo le indicazioni ricevute.

I dati devono essere trattati esclusivamente per finalità (principio della limitazione della finalità):

- **determinate** e **direttamente correlate allo svolgimento delle proprie funzioni**, non essendo consentita la raccolta fine a sé stessa;
- **esplicite**, in quanto il soggetto interessato va informato sulle finalità del trattamento;
- **legittime**, nel senso che il fine della raccolta dei dati, oltre al trattamento, deve essere lecito;
- **compatibili** con il presupposto per il quale sono inizialmente trattati, in precipuo riferimento alle finalità esplicite e determinate, specialmente per le operazioni di comunicazione e diffusione degli stessi.

I dati devono essere:

- **esatti,** ossia precisi e rispondenti al vero e, se necessario, aggiornati;
- **adeguati, pertinenti e strettamente limitati** a quanto necessario rispetto alle finalità esplicite e determinate per le quali sono trattati, in quanto devono essere raccolti solo i dati che sono al contempo strettamente necessari, sufficienti e non esuberanti in relazione ai fini, la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso (principio di minimizzazione dei dati);
- **conservati** per tutto il periodo strettamente necessario.

3. Sicurezza dei dati

3.1 Norme logistiche per l'accesso fisico ai locali

E' necessario evitare che i dati personali trattati possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Pertanto, si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro o dal luogo destinato alle riunioni collegiali della commissione, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato.

Laddove si esegue il trattamento di dati personali, deve essere possibile riporre in luogo sicuro i documenti cartacei e i supporti rimovibili contenenti tali dati. Pertanto, le porte degli uffici e almeno un armadio per ufficio devono essere dotati di serratura con chiave.

3.2 Istruzioni per l'uso degli strumenti informatici

Si fa presente che sia i dispositivi di memorizzazione del proprio PC sia le unità di rete devono contenere informazioni e dati esclusivamente collegati allo svolgimento della propria attività lavorativa e non possono essere utilizzati per scopi diversi.

3.2.1 Gestione strumenti elettronici (PC fissi e portatili)

Ciascun soggetto autorizzato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). E' tenuto a rispettare le misure di sicurezza per la tutela della riservatezza, al fine di evitare l'accesso ai dati da parte di soggetti non autorizzati.

Per la gestione della sessione di lavoro sul PC (fisso), si precisa che:

- al termine dell'orario di lavoro, il PC deve essere spento e non sarà consentito trattare i dati relativi alla procedura in argomento da luoghi diversi da quelli di lavoro (ad esempio da casa, neppure in caso di smartworking);
- se il soggetto autorizzato si assenta momentaneamente dalla propria postazione o dal luogo fissato per la riunione della commissione, deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto, deve chiudere la sessione di lavoro sul PC facendo Logout oppure deve attivare il blocco del PC (usando, ad esempio, la combinazione di tasti Win+L);
- relativamente all'utilizzo della funzione di blocco del PC, dopo un determinato periodo di inattività del PC, essa si attiva automaticamente;
- quando si esegue la stampa di un documento contenente dati personali su una stampante in rete o nel caso di trattamento dell'istanza cartacea di partecipazione, con i relativi allegati, occorre ritirare tempestivamente i documenti cartacei per evitare l'accesso a soggetti non autorizzati. In caso di stampa di documenti, è possibile attivare la funzione "stampa trattenuta" nelle proprietà "base" della stampante alla voce "lav. di stampa" che permette di non stampare il documento fino a quando l'utente non inserisca le credenziali di autenticazione.
- I documenti cartacei originali sono conservati in appositi contenitori accessibili al solo personale autorizzato e quindi archiviati a cura del Dirigente dell'Ufficio (cassaforte, armadio chiuso a chiave, etc.).

3.2.2 Gestione username e password

L'accesso al PC eventualmente utilizzato per la lavorazione delle istanze, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede al soggetto autorizzato di inserire un nome utente (username) e una parola chiave (password). L'utilizzo della combinazione username/password è fondamentale in quanto:

- tutela da accessi illeciti alla rete, ai dati e, in generale, da violazioni e danneggiamenti del patrimonio informativo;
- tutela il soggetto autorizzato da false imputazioni, garantendo che nessuno possa operare a suo nome con il suo profilo (furto identità digitale);
- è necessario per gestire correttamente gli accessi a risorse condivise.

Il Dirigente autorizza espressamente il segretario o gli altri componenti della Commissione al trattamento dati sul personal computer per le necessaria incombenze istruttorie.

Ciascun soggetto autorizzato deve scegliere la password in base ai criteri standard di sicurezza quali: combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole; diversificare dalle precedenti; effettuare un cambio frequente; conservare in luogo sicuro; non rivelare o condividere la password con i colleghi di lavoro, familiari e amici, soprattutto attraverso il telefono; non attivare la funzione che permette di salvarla e richiamarla automaticamente da alcune applicazioni.

Si raccomanda, inoltre, di non scegliere password già utilizzate per l'accesso ad altri sistemi esterni a quelli dell'Amministrazione.

3.2.3 Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione è vietata. Solo in casi particolari e motivati è possibile fare richiesta di installazione hardware e software aggiuntivo tramite i referenti informatici che inoltreranno la richiesta alla DGCASIS che ne valuterà l'opportunità.
In generale è vietato l'uso di programmi portabili (eseguibili senza installazione) e, in generale, di tutti i software non autorizzati dalla DGCASIS.
Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Nel caso in cui si renda indispensabile l'utilizzo di una o più cartelle condivise in rete tra i dipendenti di un ufficio, è necessario inoltrare richiesta alla DGCASIS, attraverso il referente informatico, e specificare nella stessa i soggetti che possono avere accesso al contenuto delle singole cartelle. Si precisa che non possono essere salvati file contenenti dati personali su cartelle condivise, salvo che non siano previsti accessi limitati ai soli soggetti autorizzati al trattamento di tali dati personali.

3.2.4 Gestione posta elettronica istituzionale

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti interni ed esterni per le finalità del MIUR.
Al fine di non compromettere la sicurezza del Sistema Informativo MIUR, occorre adottare le seguenti norme comportamentali:

- se si ricevono email da destinatari sconosciuti contenenti tipi di file sospetti, procedere alla loro immediata eliminazione;
- 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 che esulano dalla propria attività lavorativa.

Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di categorie particolari di dati, si raccomanda di prestare attenzione a che:

- il destinatario sia effettivamente competente e autorizzato a ricevere i dati inviati;
- l'indirizzo del destinatario sia stato correttamente digitato;
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.

3.2.5 Gestione del salvataggio dei dati

Per i dati e i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle condivise di rete e database, sono eseguiti i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali file distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.
Per i dati ed i documenti che risiedono esclusivamente sul PC, è opportuno effettuare copie di backup.

3.2.6 Gestione dei supporti rimovibili

I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri soggetti non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati opportunamente formattati al fine di non consentire il recupero dei dati rimossi. Il trasferimento di file contenenti dati personali su supporti rimovibili è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. Si raccomanda di proteggere con password i supporti rimovibili contenenti dati personali.

3.2.7 Protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni PC del MIUR è stato installato un software antivirus che si aggiorna automaticamente all'ultima versione disponibile.
L'antivirus non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.
Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus oppure si sospetti la presenza di un virus non rilevato dal programma antivirus, è necessario segnalarlo all'assistenza tecnica.
Si raccomanda di non scaricare e né tantomeno aprire file sospetti provenienti via email da mittenti sconosciuti. Tali file possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in esso contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

3.3 Istruzioni per l'uso degli strumenti "non elettronici"

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi. I documenti contenenti dati personali devono essere custoditi in appositi armadi o cassettiere dotate di chiavi. Tali documenti, quando si ritiene debbano essere eliminati, devono essere distrutti.
Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), nonché in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro e al termine dell'orario di lavoro.
In particolare, si richiede in ogni ufficio la presenza e l'uso tassativo di armadi e/o cassettiere dotati di serratura adeguata.
Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzano strumenti per la riproduzione cartacea di documenti digitali sono tenuti a procedere alla relativa distruzione del supporto qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie.

Il soggetto autorizzato deve attenersi alle seguenti prescrizioni:

- in nessun caso è concesso l'accesso a documentazione contenente dati personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti autorizzati;
- è severamente vietato utilizzare documenti contenenti dati personali, come carta da riciclo o da appunti;
- l'accesso ai documenti deve essere limitato al tempo necessario a svolgere i trattamenti previsti;
- il numero di copie di documenti contenenti dati personali deve essere strettamente funzionale alle esigenze di lavoro;
- ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale autorizzato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- l'accesso agli archivi deve essere controllato permettendo l'accesso ai soli soggetti autorizzati