Ministero dell'Istruzione e Del Merito
Ufficio Scolastico Regionale per il Lazio
"ISTITUTO COMPRENSIVO CIVITAVECCHIA 2"
Via F. Barbaranelli, 3/3-a - 00053 CIVITAVECCHIA (RM) Tel. 0766.031868
Cod.Fisc. 91038390588 - Cod.Mecc. RMIC8GN009 – www.iccivitavecchia2.edu.it
E-mail: rmic8gn009@istruzione.it – Pec: rmic8gn009@pec.istruzione.it

Circolare n. 92

All'Assistente Tecnico
Amministrazione Trasparente – sez. altri contenuti
Sito web

OGGETTO: AUTORIZZAZIONI ADDETTI –ASSISTENTI TECNICI - Misure finalizzate a dare attuazione alle disposizioni del Regolamento Europeo n.2016/679 e del D.lgs. n.196/03 "Codice in materia di protezione dei dati personali" e ss. mm. e ii. – Autorizzazioni Addetti al trattamento dei dati personali a.s. 2024-20245

Premesso che:

- L'Istituto Comprensivo "Civitavecchia 2 – Via Barbaranelli"- Via Barbaranelli 3-3A- 00053 Civitavecchia (RM), rappresentato dal Dirigente Scolastico Prof.ssa Francesca De Luca, è titolare del trattamento dei dati personali di alunni, genitori, personale dipendente, fornitori, e qualunque altro soggetto che abbia rapporti con l'Istituto medesimo e che a questo conferisca, volontariamente o per obbligo, propri dati personali;
- sono soggetti autorizzati al trattamento tutti i lavoratori impiegati nell'istituzione scolastica che trattano dati personali;
- l'attività di trattamento è disciplinata dal Regolamento UE 2016/679 (di seguito Regolamento), dal D.lgs.196/03 come modificato dal D.lgs.101/18 (di seguito Codice) e dalle norme di settore,
- per effetto del Regolamento il titolare del trattamento ha l'obbligo di adottare specifiche misure organizzative e di impartire istruzioni a tutti coloro che sono stati autorizzati al trattamento dei dati personali (artt.5,24,29,32);

Considerato che:

- l'autorizzazione dell'addetto non implica l'attribuzione di funzioni ulteriori rispetto a quelle già assegnate, ma consente di trattare i dati di cui si viene a conoscenza nell'esercizio di tali funzioni essendone stati autorizzati e avendo ricevuto le istruzioni sulle modalità cui attenersi nel trattamento;
- la S.V. in servizio presso questo Istituto come impiegati per lo svolgimento di servizi di carattere tecnico sui sistemi informatici dell'Istituto ed attività di laboratorio connesse alla didattica, fornendo anche supporto alle attività di carattere amministrativo, per l'espletamento delle Loro funzioni, hanno necessità di venire a conoscenza e di trattare dati personali, fermi restando gli obblighi e le responsabilità civili e penali;

Tutto ciò premesso,
l'Istituto Comprensivo "Civitavecchia 2 – Via Barbaranelli"- Via Barbaranelli 3-3A 00053 Civitavecchia (RM), rappresentato dal Dirigente Scolastico Prof.ssa Francesca De Luca, autorizza la S.V. al trattamento dei dati personali. La presente autorizzazione ha effetto esclusivamente in relazione all'ambito del trattamento e alle banche dati di cui agli allegati. Il trattamento dei dati personali consentito alla S.V. è strettamente limitato a quanto necessario ed indispensabile all'adempimento delle proprie mansioni, osservando inderogabilmente le norme di legge, i regolamenti interni, circolari, ordini di servizio, il manuale sulla sicurezza ad uso degli autorizzati al trattamento dei dati, alle istruzioni comunque impartite dal titolare del trattamento e dei suoi delegati. La S.V. è altresì tenuta a seguire i corsi di formazione in materia di disciplina della protezione dei dati. Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto sono dovuti in base al vigente CCNL. Nel caso di inadempimento si applicheranno le sanzioni disciplinari previste dal vigente CCNL. La presente autorizzazione ha efficacia fino alla risoluzione del rapporto di lavoro per qualsiasi causa oppure fino a modifica o revoca da parte del Titolare del trattamento. A titolo di documentazione amministrativa si chiede di firmare per ricevuta la seguente comunicazione.

Il Titolare del trattamento
Istituto Comprensivo "Civitavecchia 2 – Via Barbaranelli"

Il Dirigente Scolastico
Prof.ssa Francesca De Luca

Firmato dal Dirigente Scolastico
Prof.ssa Francesca De Luca
20/11/2024 14:05:12

Allegato A - Ambito di trattamento consentito

In qualità di impiegati dell'Istituzione scolastica, svolgendo con autonomia operativa e responsabilità servizi di carattere tecnico di assistenza e manutenzione ordinaria del sistema informatico dell'Istituto, ed attività di laboratorio connesse alla didattica, fornendo anche supporto alle attività di carattere amministrativo, secondo quanto previsto nel relativo profilo di Area del personale ATA – Assistente Tecnico allegato al CCNL, la S.V. necessariamente partecipa a trattamenti di dati personali, riguardanti le operazioni specifiche svolte nell'area di attività nella quale è impegnata e nell'ambito delle sue competenze professionali.
La S.V. è pertanto autorizzata ai trattamenti dei dati personali anche appartenenti a particolari categorie (ai sensi dell'art.9 del Regolamento UE), riferiti a tutti i soggetti con i quali l'Istituzione Scolastica entra in relazione per i suoi fini istituzionali, nella misura e nei limiti stabiliti dal Regolamento, dal Codice e dal Regolamento recante "l'identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione" (D.M. n.305 del 07.12.06).

Allegato B - Banche Dati

Nello svolgimento dell'attività lavorativa gli addetti autorizzati potranno effettuare le operazioni di trattamento dei dati personali riguardanti le Aree: Alunni, personale e contabile amministrativa e connesse all'esecuzione dei servizi tecnici di assistenza e manutenzione dei sistemi informatici ed all'attività di supporto alla didattica ed alla segreteria amministrativa.
I dati personali trattati dagli assistenti tecnici sono contenuti sia in banche dati su supporto cartaceo, che in archivi elettronici e digitali, e possono riguardare, limitatamente alla conoscenza necessaria allo svolgimento delle proprie mansioni di supporto ai sistemi informatici dell'Istituto ed allo svolgimento delle attività didattiche di laboratorio:

- dati personali di alunni e rispettive famiglie utilizzabili per finalità didattiche da docenti;
- materiale didattico e valutazioni inerenti alle attività di laboratorio, secondo le direttive fornite dal docente di laboratorio;
- dati personali di alunni e genitori utilizzabili per finalità amministrative, gestionali e di raccordo fra le diverse strutture operative;
- dati personali contenuti nelle pratiche di acquisto e forniture di beni e servizi e rapporti con i fornitori, per quanto riguarda la manutenzione e la dotazione delle apparecchiature tecniche ed informatiche, nonché degli uffici;
- dati personali del personale alle dipendenze ed in collaborazione contenuti nelle pratiche amministrative e contabili, gestione finanziaria e bilancio;
- dati personali contenuti nei documenti protocollati o necessari per lo svolgimento delle attività istituzionali.

Il trattamento dei dati personali può riguardare le seguenti operazioni applicate ai dati: raccolta, registrazione, organizzazione, conservazione, modifica, consultazione, comunicazione, diffusione, raffronto, cancellazione.

Allegato C - Istruzioni specifiche sul trattamento dei dati personali

Nel precisare che gli indirizzi operativi sinora forniti risultano coerenti con finalità e metodi cui la suddetta normativa privacy (Regolamento UE n.2017/679, D.lgs. n. 196/03 e ss. mm. e ii. e Decreto legislativo 10 agosto 2018, n.101) riconosce legittimità, si intende con la presente indicare formalmente le istruzioni operative che la S.V. dovrà comunque continuare a rispettare rigorosamente nel trattamento dei dati personali:

1. Il trattamento dei dati personali deve avvenire ai sensi della normativa privacy vigente, in modo lecito e secondo correttezza, e seguendo le direttive impartite dal titolare del trattamento;
2. Il trattamento dei dati personali è consentito solo per lo svolgimento delle funzioni istituzionali della Scuola;
3. I soggetti autorizzati potranno raccogliere e registrare i dati personali esclusivamente per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
4. Gli addetti autorizzati acquisiranno solo dati necessari e sufficienti per le finalità cui è preposta la propria unità lavorativa;
5. Gli addetti autorizzati potranno conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati ed eserciteranno altresì la dovuta diligenza affinché non vengano conservati, nel proprio settore operativo, dati non necessari o divenuti ormai superflui;
6. Gli addetti autorizzati dovranno mantenere assoluto riserbo sui dati personali di cui verranno a conoscenza nell'esercizio delle loro attività;
7. L'obbligo di mantenere la dovuta riservatezza in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico ricoperto presso questa istituzione scolastica, deve permanere in ogni caso, anche quando sia venuto meno l'incarico stesso;
8. I soggetti autorizzati, nell'ambito delle proprie attribuzioni lavorative, cureranno l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati, verificando inoltre che questi ultimi siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali essi stessi sono stati raccolti e successivamente trattati;
9. Nello svolgimento dell'attività lavorativa gli addetti autorizzati potranno effettuare le operazioni di trattamento dei dati personali descritte nel presente documento (Allegato A) ed individuate nel "Registro dei trattamenti" dell'Istituto;

10. Gli addetti autorizzati avranno cura, secondo le comuni regole della prudenza e della diligenza, di trattare i dati stessi con la massima riservatezza e di impedire, per quanto possibile, che estranei non autorizzati prendano conoscenza dei dati che loro mantengano all'esclusivo fine lavorativo;
11. In ogni operazione di trattamento andrà garantita la massima riservatezza e custodia degli atti e dei documenti contenenti dati personali, che devono essere mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate ad accedervi a prenderne visione o ad effettuare qualsivoglia trattamento;
12. L'accesso agi archivi contenenti dati particolari (ex sensibili e giudiziari) è consentito solo alle persone autorizzate ed è soggetto a continuo controllo secondo le misure di sicurezza predisposte dall'Istituzione scolastica;
13. In caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'addetto autorizzato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non autorizzati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento - a tal fine, tra l'altro, l'addetto autorizzato deve assicurarsi sistematicamente che, i contenitori degli archivi e banche dati (scrivanie, cassetti, armadi, computer fissi, laptop, tablet, etc.) siano chiusi a chiave e/o protetti da password (nel caso in cui il trattamento venga effettuato con strumenti elettronici e sistemi ICT) e che i dati dagli stessi estratti non possano divenire oggetto di trattamento improprio;
14. I soggetti autorizzati potranno comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ad altri soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute dal titolare del trattamento;
15. È vietata qualsiasi forma di diffusione e comunicazione dei dati personali trattati che, essendo strettamente funzionale allo svolgimento dei compiti affidati, non sia stata appositamente autorizzata dal Titolare del trattamento;
16. Le comunicazioni anche verbali e/o telefoniche agli interessati dovranno avvenire in forma riservata- se effettuate per scritto dovranno essere consegnate in contenitori chiusi;
17. In caso di trasmissione di documenti contenenti dati personali l'addetto autorizzato si dovrà assicurare dell'identità dell'interessato che li riceve o di chi è stato delegato al ritiro del documento in forma scritta;
18. In caso di comunicazioni elettroniche ad alunni, colleghi, genitori, personale della scuola o altri soggetti coinvolti per finalità istituzionali, queste (comunicazioni) vanno poste in essere seguendo le indicazioni fornite dall'Istituzione scolastica e avendo presente la necessaria riservatezza delle comunicazioni stesse e dei dati coinvolti;
19. Al termine del trattamento gli addetti autorizzati dovranno assicurarsi che gli atti e i documenti contenenti dati appartenenti a particolari categorie e relativi a condanne e reati, vengano conservati in contenitori muniti di serratura o in ambienti ad accesso selezionato e vigilato, fino alla restituzione;
20. Al termine del trattamento, eventuali fogli a stampa o compilati a mano che siano stati prodotti e/o utilizzati nella fase istruttoria o preparatoria, qualora contenenti dati personali, devono essere distrutti e resi illeggibili;
21. Ai soggetti autorizzati non è consentito asportare supporti informatici o cartacei né copiare documenti, contenenti dati personali di terzi, senza la previa autorizzazione del titolare del trattamento;
22. Eventuali supporti removibili utilizzati (es. chiavi USB, hard disk portatili, ecc.) su cui sono memorizzati dati personali vanno custoditi con cura e non devono essere messi a disposizione o lasciati al libero accesso di terzi non autorizzati;
23. Supporti removibili contenenti dati particolari (ex sensibili e giudiziari), se non utilizzati, vanno distrutti o resi inutilizzabili mediante apposite tecniche di cancellazione sicura dei dati, di formattazione e di distruzione, effettuate da operatori specializzati;
24. Gli autorizzati saranno tenuti a rispettare ed applicare le misure di sicurezza idonee a salvaguardare la riservatezza e l'integrità dei dati, adottate dall'Istituto ed indicate nelle "Linee Guida "per il trattamento dei dati personali.

Le stesse norme si applicano obbligatoriamente al trattamento di dati personali contenuti in un archivio o destinati a figurarvi e si differenziano in base alle modalità di trattamento, ovvero se il trattamento dei dati possa essere effettuato in formato digitale (con l'ausilio di strumenti informatici e tecnologie innovative per la didattica) o cartaceo (senza l'ausilio di strumenti informatici). Pertanto si riportano ulteriori istruzioni che dovranno essere seguite nell'esecuzione di determinate operazioni effettuate sugli archivi di dati cartacei e digitali, sugli strumenti ed applicativi in dotazione, sui servizi internet ad uso lavorativo ed in determinate condizioni in cui viene prestata l'attività professionale.

Archivi cartacei di dati personali

L'archivio cartaceo viene comunque gestito nel pieno rispetto delle idonee misure di sicurezza in relazione al tipo di documentazione in esso contenuta. Gli eventuali atti e documenti contenenti dati personali compresi nelle particolari categorie e relativi a vicende giudiziarie sono affidati ai soggetti autorizzati per lo svolgimento dei relativi compiti; i medesimi atti e documenti sono controllati e custoditi dagli autorizzati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate. L'accesso agli archivi contenenti dati di particolari categorie e/o giudiziari è controllato e consentito solo agli addetti espressamente autorizzati.
Gli archivi cartacei vengono gestiti secondo le seguenti modalità:

- possono accedere alle informazioni contenute nell'archivio cartaceo solo gli addetti autorizzati

- l'accesso alle informazioni è consentito limitatamente ai soli dati personali la cui conoscenza è strettamente necessaria per lo svolgimento dei compiti assegnati;
- tutti i documenti che contengono dati personali sono conservati in archivi ad accesso selezionato;
- i documenti contenenti dati personali non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali e, nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento;
- i faldoni contenenti i dati sono archiviati in una forma che non consenta l'identificazione dell'interessato a chi non autorizzato e comunque per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti e successivamente trattati;
- per tutto il periodo in cui i documenti che contengono dati personali sono al di fuori dei locali individuati per la loro conservazione, gli addetti autorizzati non dovranno lasciarli mai incustoditi, adottando ogni cautela affinché ogni persona non autorizzata non venga a conoscenza del contenuto;
- al termine dell'orario di lavoro tutti i documenti che contengono dati personali devono essere riportati nei locali individuati per la loro conservazione;
- per evitare il rischio di diffusione dei dati personali si deve limitare l'utilizzo di copie fotostatiche ed è vietato utilizzare copie fotostatiche di documenti che contengono dati personali all'esterno del luogo di lavoro.

Gestione archivi digitali e documenti informatici contenenti dati personali

- UTILIZZO DELLE CREDENZIALI DI AUTENTICAZIONE
  - L'accesso alle procedure informatiche che trattano dati personali è consentito solo agli Incaricati in possesso di "credenziali di autenticazione" che permettano il superamento di una procedura di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (user-id) associato ad una parola chiave riservata (password) e/o in un dispositivo di autenticazione o in una caratteristica biometrica
  - Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
  - Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato
  - Gli addetti devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle istruzioni contenute nelle linee guida (LG) e nel manuale operativo ad uso degli addetti autorizzati (IS01 – Istruzioni operative addetti)

- PROTEZIONE DEL PC E DEI DATI
  - Tutti i PC devono essere dotati di password rispondenti alle policy interne
  - Tutti i PC devono essere dotati di software antivirus aggiornato costantemente e con la funzione "Monitor" attiva
  - Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa, dotati di licenza e forniti dalla Scuola
  - Sono vietati i software scaricati da Internet o acquisiti autonomamente
  - Per evitare accessi illeciti, deve essere sempre attivato il salva schermo con password
  - Sui PC devono essere installati, appena vengono resi disponibili (e comunque almeno annualmente), tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti
  - Deve essere effettuato, con cadenza almeno settimanale un salvataggio di back-up di eventuali dati personali salvati in locale, presenti sul proprio PC personale o non condivisi tramite il server della Scuola
  - I supporti di memoria utilizzati per il back-up devono essere trattati secondo le regole definite al punto "Archivi cartacei di dati personali"
  - I supporti rimovibili contenenti dati di particolari categorie e/o giudiziari se non utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri addetti, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

- CANCELLAZIONE DEI DATI DAI PC
  - I dati personali conservati sui PC devono essere cancellati in modo sicuro, con tecniche efficaci effettuate ad opera del personale tecnico specializzato, prima di destinare i PC ad usi diversi

Come comportarsi in presenza di ospiti o di personale di servizio

- Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali
- Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti, non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento e attivare il salvaschermo del PC
- Non rivelare o fare digitare le password dal personale di assistenza tecnica
- Non rivelare a nessuno le password - nessuno è autorizzato a chiederle
- Segnalare qualsiasi anomalia o situazione di pericolo per i dati trattati al titolare

Regole generali per le password

Ciascun addetto Autorizzato è in possesso di diverse credenziali di autenticazione, costituite da username e password (autenticazione semplice), per accedere ai servizi informatici istituzionali o su internet, che dovrà utilizzare e gestire attenendosi alle seguenti istruzioni. Le credenziali di autenticazione in generale consentono all'addetto autorizzato l'accesso ad un computer o ad una rete, esse sono individuali e pertanto non vanno mai condivise con altri utenti (anche se autorizzati). La password deve essere composta da almeno otto caratteri, anche se più aumenta il numero dei caratteri più la password diventa "robusta" (si suggerisce intorno ai 15 caratteri), non deve essere riconducibile alla propria persona o contenere parole di uso comune (facili da indovinare) e deve essere cambiata da ciascun autorizzato almeno ogni 3 mesi. Per evitare accessi illeciti, al termine di ciascun trattamento l'addetto autorizzato dovrà uscire dall'applicazione utilizzata assicurandosi di avere eseguito il logout.

Posta elettronica ed internet

- Gli strumenti digitali ufficiali per la condivisione dei materiali tra colleghi sono gli account e le mail istituzionali e non account e indirizzi e-mail personali, che possono essere utilizzati solo in ambito non lavorativo per scopi personali;
- non è consentito utilizzare la posta elettronica istituzionale e le piattaforme dedicate allo svolgimento delle attività lavorative (in particolare videocomunicazioni e riunioni di lavoro n videoconferenza) per motivi non attinenti allo svolgimento delle mansioni assegnate;
- non utilizzare la posta elettronica per comunicare informazioni riservate, dati personali anche sensibili senza l'autorizzazione del titolare e/o del responsabile e senza garantirne l'idonea protezione - la posta elettronica può usata per inviare messaggi contenenti dati appartenenti a particolari categorie ai sensi dell'art.9 del Regolamento UE 2016/679, solo previa crittografia dei dati o dell'intero documento che li contiene - una volta cifrati, i dati possono essere decifrati soltanto da utenti che dispongono della chiave crittografica appropriata (ad esempio una password);
- fare attenzione ai messaggi di posta elettronica verificandone la provenienza in quanto, essi rappresentano uno dei metodi più subdoli per veicolare contenuti di virus, worm e frodi (anche senza necessità di allegati), malware anche in grado di cancellare i dati o renderli indisponibili, in particolare non aprendo e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio un mittente o natura dell'oggetto poco chiari) e non cliccando su eventuali link inseriti nella missiva;
- accertarsi sempre che i destinatari siano autorizzati ad entrare in possesso dei dati oggetto della comunicazione;
- non rispondere ai messaggi di posta elettronica provenienti da indirizzi non noti;
- non comunicare la propria e-mail istituzionale a siti, che hanno scarsa attinenza con l'attività e verso i quali non si ha interesse e/o sui quali si nutre il minimo dubbio riguardo alla loro attendibilità;

Inoltre, nell'utilizzo degli strumenti in dotazione (apparecchiature informatiche e connessioni alla rete scolastica) adottare le seguenti misure:

- Accedere solo ai siti i cui contenuti siano correlati all'attività lavorativa - è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- durante la navigazione, prima di selezionare un link, fare attenzione a tutti i messaggi provenienti dal browser che richiedono l'apertura, l'installazione o il salvataggio di files.
- non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal titolare;
- non è consentito lo scarico di software gratuiti (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal titolare;
- non è permessa la partecipazione, per motivi non professionali a Forum, l'utilizzo di chat line, social network, ecc., anche utilizzando pseudonimi (o nickname);
- è severamente vietato aggirare le protezioni applicate ai sistemi informatici con software capace di farlo.

Civitavecchia 20/11/2024