



MINISTERO DELL'ISTRUZIONE
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
POLO TECNICO-PROFESSIONALE "GALILEO"
I.I.S. "CARLO URBANI"

Uffici di Presidenza e Segreteria: Via dell'Idroscalo, 88 - 00121 Roma - Municipio X - Distretto XXI - Ambito X - Cod. IPA istsc_rmiso03300b
Codice Istituzione RMISO3300B - *Codice fiscale* 97196850586 - *Conto corrente postale* 25157025 - *Cod. Fattura Elettronica* UFZFN8

Sito Istituto: www.istitutocarlobarbani.edu.it

E-mail: ✉ rmiso3300b@istruzione.it - ✉ rmiso3300b@pec.istruzione.it -

SEDE ASSOCIATA DI OSTIA: Via dell'Idroscalo, 88 - 00121 Roma - ☎ 06.12.11.26.360 ☎ 06.12.11.26.361

SEDE ASSOCIATA DI ACILIA: Via di Saponara, 760 - 00125 Roma ☎ 06/12.11.25.325

ISTITUTO PROFESSIONALE: Servizi Commerciali - Design per la Comunicazione Visiva e Pubblicitaria /Odontotecnico / Industria e Artigianato per il Made in Italy: Grafica Industry 4.0

ISTITUTO TECNICO: Grafica e Comunicazione - **LICEO DELLE SCIENZE UMANE:** opzione Economico Sociale

Prot. n. 902 - 7.6
Roma, li 01 settembre 2022

Al Personale ATA – Assistenti Tecnici
Sito web Sezione Privacy

**Oggetto: Protezione dei Dati Personali ai sensi ex D.lgs. 196/2003 e ex Regolamento UE 679/2016 -
Nomina Assistenti Tecnici Incaricati del Trattamento dati personali**

IL DIRIGENTE SCOLASTICO

- VISTO** il Regolamento UE 679/2016;
- VISTO** il Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", (indicato di seguito come Codice)
- PRESO ATTO** che la titolarità del trattamento dei dati personali di alunni, genitori, personale dipendente, fornitori, e qualunque altro soggetto che abbia rapporti con questo Istituto Scolastico e che a questo conferisca, volontariamente o per obbligo, propri dati personali è in capo al Dirigente Scolastico in qualità di legale rappresentante pro tempore dello stesso;
- PRESO ATTO** che è stato designato Responsabile Interno del Trattamento dei Dati in questo Istituto Scolastico il DSGA, Sig.a Angela MELIS, per profilo professionale, funzione rivestita, esperienza, capacità ed affidabilità fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza
- SENTITO** il DSGA quale Responsabile interno del Trattamento Dati;
- CONSIDERATO** che il Dirigente scolastico in qualità di rappresentante legale pro tempore dell'Istituzione scolastica esercita la titolarità del trattamento dei dati personali;
- CONSIDERATO** che il Direttore dei Servizi Generali ed amministrativi (DSGA), per profilo professionale, funzione rivestita, esperienza, capacità ed affidabilità fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza;
- RILEVATO** che in qualità di assistente tecnico dell'Istituzione scolastica, le SS.VV. partecipano sia a trattamenti di dati personali (intesi nell'ampia accezione di cui agli artt. da 1 a 6 del Regolamento UE n.2016/679), riguardanti le operazioni specifiche svolte nell'area di attività nella quale è impegnata e nell'ambito delle Sue competenze professionali, sia, talvolta all'accesso ed al trattamento dei dati personali particolari quali indicati negli artt. 9-10 del Regolamento UE n. 2016/679), riguardanti tutti i soggetti con i quali l'Istituzione scolastica entra in relazione per i suoi fini istituzionali;

PREMESSO che la nomina ad incaricato non implica l’attribuzione di funzioni ulteriori rispetto a quelle già assegnate alla S.V., che consistono nella collaborazione con il corpo docente per le attività di laboratorio, eventuali interventi di assistenza e manutenzione ordinaria del sistema informatico dell’Istituto e rapporti con i fornitori, bensì, l’espletamento delle anzidette funzioni ai sensi e per gli effetti del Regolamento UE n.2017/679, precisando, peraltro che gli indirizzi operativi sinora fornitile risultano coerenti con finalità e metodi cui al Regolamento UE n.2016/679 ;

DESIGNA

il personale in indirizzo

INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

il quale SI IMPEGNA

- a procedere al trattamento dei dati personali nel rispetto dei principi generali di cui al Regolamento Europeo 679/2016 per scopi determinati, espliciti e legittimi tenendo presente che i dati devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- a rispettare i divieti di comunicazione e diffusione dei dati trattati nel corso del presente incarico e a non utilizzare i dati, cui abbia accesso, per finalità incompatibili con quelle relative al profilo di appartenenza. Si ricorda che le operazioni di comunicazione e diffusione dei Dati Personali Particolari indicati negli art. 9 e 10 del Regolamento Europeo 679 /2016 sono possibili quando vi sia una apposita previsione di legge o di regolamento,
- ad attenersi, nel suo operato, alle istruzioni ricevute per lo svolgimento delle operazioni di trattamento;
- nello specifico, gli assistenti tecnici informatici sono inoltre autorizzato ad intervenire sui PC dell’Amministrazione per garantire un servizio di assistenza e manutenzione ordinaria del sistema informatico dell’Istituto, ivi compresi i PC della segreteria in cui avviene il trattamento di dati personali. Nello svolgimento di tale attività la S.V. dovrà:
 - evitare qualunque accesso ai dati personali presenti nei PC a meno che questo non sia tecnicamente necessario allo svolgimento del compito ricevuto,
 - provvedere all’effettuazione preventiva della copia di sicurezza dei dati ogni qualvolta l’intervento tecnico comporti il rischio della perdita dei dati;
- garantire la riservatezza e l’integrità dei dati personali trattati nello svolgimento dell’attività di assistenza tecnica e manutenzione;
- rispettare i divieti di comunicazione e diffusione dei dati trattati nel corso del presente incarico e a non utilizzare i dati, cui abbia accesso, per finalità incompatibili con quelle relative al profilo di appartenenza.

La presente nomina di Incaricato al trattamento dei dati personali è a tempo indeterminato e può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati personali senza preavviso. La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa Istituzione Scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro. Successivamente a tale data, la S,V. non sarà più autorizzata ad effettuare alcun tipo di trattamento di dati per conto di questa Istituzione Scolastica.

L’Incaricato nell’espletamento delle sue mansioni dovrà attenersi scrupolosamente alle sotto indicate ISTRUZIONI SPECIFICHE.

1 . Trattamenti eseguiti con supporto cartaceo:

- a) controllare e custodire gli atti e i documenti contenenti dati personali in modo da assicurarne l’integrità e la riservatezza;
- b) conservare sempre i dati del cui trattamento si è incaricati in apposito armadio assegnato;
- c) accertarsi della corretta funzionalità dei meccanismi di chiusura degli armadi, segnalando tempestivamente al Responsabile eventuali anomalie;
- d) fornire sempre l’informativa all’interessato o alla persona presso cui si raccolgono i dati prima di

**ISTITUTO DI ISTRUZIONE SUPERIORE “CARLO URBANI”
ROMA**

- procedere alla raccolta e al trattamento dei dati;
- e) consegnare, quando necessario, il modulo per il consenso da parte dell'interessato. Ricevere quindi il modello opportunamente firmato da parte dell'interessato o di chi lo rappresenti;
 - f) limitare l'accesso ai dati personali, oggetto di trattamento, la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità di cui al provvedimento di incarico;
 - g) conservare i documenti o atti che contengono dati sensibili o giudiziari in archivi (ad esempio stanze, armadi, schedari, contenitori in genere) chiusi a chiave;
 - h) Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Responsabile;
 - i) richiedere l'identità del chiamante e quindi provvedere a richiamare, avendo così la certezza sull'identità del richiedente, qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia;
 - j) non fornire telefonicamente o a mezzo PEO-PEC dati e informazioni ai diretti interessati senza avere la certezza della sua identità;
 - k) inviare a mezzo PEO-PEC documenti in chiaro contenenti dati sensibili solo utilizzando la mail istituzionale;
 - l) distruggere o comunque rendere illeggibili, prima di essere eliminati o cestinati i documenti cartacei non più utilizzati, specie se contenenti dati sensibili;
 - m) vietare l'accesso a estranei e a soggetti non autorizzati alle aree in cui sono conservati dati personali su supporto cartaceo;
 - n) conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti;
 - o) consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti;
 - p) Vietare l'accesso a estranei al fax e alla stampante che contengano documenti non ancora ritirati dal personale;
 - q) effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;
 - r) non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte;
 - s) non lasciare incustodito, se esistente, il registro contenente gli indirizzi e i recapiti telefonici del personale e degli studenti e non annotarne il contenuto sui fogli di lavoro;
 - t) non lasciare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati;
 - u) segnalare tempestivamente al Responsabile la presenza di documenti incustoditi provvedendo temporaneamente alla loro custodia;
 - v) attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal Responsabile o dal Titolare

2. Trattamenti eseguiti con supporto informatico:

- a. utilizzare le parole chiave definite dal Responsabile della gestione e della manutenzione del sistema informatico e alle quali sono associati le relative autorizzazioni per l'accesso al sistema informatico;
- b. adottare le necessarie cautele per assicurare la segretezza della parola chiave e la diligente custodia di ogni altro dispositivo di autenticazione informatica (badge, schede magnetiche, chiavi USB, etc.)
- c. E' fatto divieto comunicare a qualunque altro incaricato le proprie credenziali di accesso al sistema informatico;
- d. modificare almeno ogni sei mesi (tre mesi nel caso di dati sensibili) la parola chiave, che viene assegnata dal Responsabile del trattamento o dal Responsabile della gestione e della manutenzione del sistema informatico. La parola chiave da consegnare deve essere chiusa in una busta opaca, sigillata e controfirmata sui lembi;

**ISTITUTO DI ISTRUZIONE SUPERIORE “CARLO URBANI”
ROMA**

- e. Prevedere che soltanto il Responsabile abbia la possibilità, previa comunicazione all'incaricato, di aprire la busta, per esigenze operative o di organizzazione. L'incaricato nel tal caso provvederà a sostituire la parola chiave violata;
- f. provvedere a porre i pc e/o i terminali in condizione di non essere utilizzati da terzi estranei tutte le volte che si lascia incustodita la propria postazione di lavoro. In particolare si chiudano tutte le applicazioni in uso e si ponga un blocco del sistema mediante password; installare sullo schermo dei pc lo screen saver con password.
- g. spegnere sempre il PC alla fine della giornata lavorativa o in caso di assenze prolungate dalla postazione di lavoro;
- h. dare immediata comunicazione al Responsabile del Trattamento su difformità dei dati trattati o del funzionamento degli elaboratori
- i. riutilizzare i supporti informatici, già utilizzati per il trattamento dei dati sensibili e giudiziari, solo se le informazioni precedentemente contenute non sono più in alcun modo recuperabili, dovendo altrimenti essere distrutti;
- j. utilizzare l'antivirus per la verifica di ogni documento trattato o di qualunque file scaricato da Internet;
- k. utilizzare sempre l'antivirus per verificare il contenuto di qualunque supporto di memorizzazione sospetto;
- l. aggiornare con frequenza l'antivirus e comunicare al Responsabile del trattamento dei dati ogni problema a riguardo;
- m. informare il Responsabile del trattamento se l'antivirus riscontra la presenza di un virus informatico;
- n. non installare sui PC alcun software senza l'autorizzazione del Responsabile del trattamento.
- o. È vietato modificare le impostazioni effettuate sul sistema dal Responsabile della gestione e della manutenzione del sistema informatico.

3. Regole per la scelta delle parole chiave

- a) usare una parola chiave di almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, costituita da un numero di caratteri pari al massimo consentito;
- b) la parola chiave non deve contenere riferimenti facilmente riconducibili all'incaricato (come per esempio nome, cognome, data di nascita, numeri di telefono, etc. propri o dei propri familiari);
- c) usare una combinazione di caratteri alfabetici e numerici, meglio se contenente almeno un segno di interpunzione o un carattere speciale;
- d) conservare con cura la parola chiave evitando di trascriverla su fogli posti in vista in prossimità del PC o sulla rubrica dell'ufficio.

In coda ad ogni messaggio in uscita da PEO / PEC si deve inserire la seguente dicitura:

AVVERTENZE AI SENSI DEL D.Lgs. 196/2003

Le informazioni contenute in questo messaggio di posta elettronica e/o nel/i file/s allegato/i sono da considerarsi strettamente riservate.

Il loro utilizzo è consentito esclusivamente ai destinatari del messaggio, per le finalità indicate nel messaggio stesso.

Qualora riceviate questo messaggio senza esserne i destinatari, Vi preghiamo cortesemente di darcene notizia via e-mail (anche all'indirizzo rmis03300b@istruzione.it) e di procedere alla immediata distruzione del messaggio stesso, cancellandolo dal Vostro sistema.

Conservare il messaggio stesso, divulgarlo anche in parte, distribuirlo ad altri soggetti, copiarlo, od utilizzarlo per finalità diverse, costituisce comportamento contrario ai principi dettati dal D.Lgs. 196/2003

This e-mail (including attachments) is intended only for recipients named above.

It may contain confidential or privileged information and should not be read, copied or otherwise used by any other person.

If you are not the named recipient, please contact rmis03300b@istruzione.it and delete the e-mail from your system.

Rif. DL 196/03.

**ISTITUTO DI ISTRUZIONE SUPERIORE “CARLO URBANI”
ROMA**

Per le misure minime di sicurezza informatica nelle PA si rimanda alle indicazioni dell'AgID:

<https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict>

Le disposizioni descritte nel presente documento potranno essere modificate e/o integrate in funzione di aggiornamenti normativi.



IL DIRIGENTE SCOLASTICO

Prof.ssa Rosa Caccioppo

*Firma autografa sostituita a mezzo stampa
art. 3 comma 2 del D.Lgs n. 1993*