



DIREZIONE DIDATTICA STATALE  
2° CIRCOLO "E. Celentano" - POMPEI -  
Via Civita Giuliana n. 26 - ☎ 081/8506209 - telefax 081/8506929  
Codice Scuola : NAEE220002 - C.F. 82015230632  
Posta ordinaria: [naee220002@istruzione.it](mailto:naee220002@istruzione.it)  
Posta PEC: [naee220002@pec.istruzione.it](mailto:naee220002@pec.istruzione.it)  
Sito WEB: [www.pompeisecondocircolo.edu.it](http://www.pompeisecondocircolo.edu.it)  
Codice univoco IPA: UFJ5EVW

Prot. 7457 / A39

Pompei, 10/11/2021

- Agli Incaricati Trattamento dati Personali  
-Sito Web

## Istruzioni per gli incaricati al trattamento dei dati

Regolamento Europeo 2016/679

Ai sensi del Regolamento UE 2016/679 di seguito indicato come "Regolamento" e delle disposizioni del D. Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" (novellato dal D. Lgs 10 agosto 2018 n. 101) lo scrivente Istituto, in qualità di Titolare del trattamento, ha elaborato per i propri incaricati le seguenti istruzioni circa il trattamento dei dati personali da effettuarsi durante l'espletamento delle proprie funzioni:

### 1. Trattamento dei dati personali

Gli incaricati sono autorizzati ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione tramite lettera di incarico, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati aziendali che contengono i predetti dati personali.

Il trattamento deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate dal Titolare e, pertanto, in conformità alle informazioni che il Titolare ha comunicato agli interessati.

Circa le modalità del trattamento si richiama la necessità di prestare particolare attenzione all'esattezza dei dati trattati e di provvedere inoltre, se di propria competenza, all'aggiornamento degli stessi.

Si ricorda che le norme sulla privacy si applicano alle sole persone fisiche.

### 2. Creazione di nuove banche dati

Senza preventiva autorizzazione non è permesso realizzare nuove ed autonome banche dati contenenti dati personali, secondo criteri organizzativi e/o per finalità diverse da quelle già previste.

### 3. Raccolta dei dati

#### 3.1 Dati personali particolari (dipendenti, fornitori, alunni)

All'atto della raccolta dei dati occorrerà fornire l'informativa sul trattamento dei dati personali, secondo le indicazioni e in conformità ai modelli elaborati dall'Istituto, avendo cura inoltre di raccogliere il consenso ove ciò risulti necessario. L'incaricato dovrà conservare la copia del consenso espresso dall'interessato.

L'incaricato non può iniziare nessun trattamento dei dati senza previo consenso dell'interessato.

Tutti i documenti vanno conservati in un luogo protetto ad accesso controllato (per esempio armadio chiuso a chiave).

#### 3.2 Disposizioni generali

Qualora l'incaricato ritenga necessario, per esigenze legate alla mansione, effettuare un trattamento diverso (sotto il profilo delle finalità, dei dati trattati, dell'ambito di comunicazione o diffusione) rispetto a quelli riportati nell'informativa agli interessati occorre rapportarsi preventivamente con il responsabile del trattamento o in alternativa con referente, al fine di individuare la necessità del trattamento medesimo e gli obblighi conseguenti.

#### **4. Comunicazione e diffusione dei dati**

Si precisa ulteriormente che è autorizzata la comunicazione dei dati personali esclusivamente ai soggetti individuati nelle informative resa agli interessati, per le finalità ivi indicate, e in relazione ai quali è stato espresso il consenso se necessario. Ogni ipotesi diversa di comunicazione o, addirittura, di diffusione dei dati dovrà essere preventivamente autorizzata di volta in volta dal Titolare; l'incaricato, prima di procedere alla comunicazione/diffusione dovrà quindi rapportarsi con il responsabile del trattamento o con il referente.

#### **5. Diritti degli interessati**

Gli incaricati sono tenuti ad effettuare il riscontro dei diritti degli interessati (indicare le misure organizzative in attuazione degli art. dal 15 al 21 del codice)

#### **6. Trattamento con strumenti elettronici - misure di sicurezza**

Ogni incaricato è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito, già predisposte dal Titolare, nonché quelle che in futuro verranno comunicate. In particolare è previsto quanto segue:

Il trattamento dei dati personali può avvenire con strumenti elettronici (informatici).

Per ogni incaricato sono previste le seguenti misure di sicurezza:

- è assegnata in via riservata la credenziale di autenticazione che consente l'accesso ai dati, attraverso una procedura di autenticazione;
- la credenziale per l'autenticazione consiste nell'associazione di un codice identificativo (utente) attribuito individualmente e di una parola chiave riservata (password);
- ciascun incaricato, per accedere ai dati ed effettuare il trattamento, deve utilizzare esclusivamente la credenziale a lui assegnata;
- la parola chiave (password):
  - non va comunicata ad altri incaricati e non va annotata su biglietti di carta, post-it lasciati poi incustoditi (la soluzione migliore è memorizzarla);
  - deve essere composta da almeno otto caratteri;
  - non deve contenere riferimenti agevolmente riconducibili all'incaricato (evitare date di nascita, nomi di figli o di coniuge, ecc.);
  - deve essere autonomamente modificata dallo stesso incaricato immediatamente in occasione del primo utilizzo, e successivamente ogni 6 mesi, ogni 3 mesi nel caso di trattamento di dati sensibili o giudiziari;

La gestione della propria postazione informatica assegnata è soggetta alle seguenti prescrizioni:

- non va lasciata incustodita lasciando accessibili i dati, quindi quando l'incaricato si allontana dalla postazione deve azionare un salvaschermo protetto dalla parola chiave o utilizzare una funzione di blocco temporaneo del computer;
- tutti i supporti magnetici utilizzati vanno riposti negli archivi (e opportunamente chiusi a chiave nel caso di dati sensibili);
- i supporti non più utilizzati possono essere eliminati solo dopo che i dati contenuti sono stati resi effettivamente inutilizzabili tramite una procedura di formattazione che non renda leggibili i dati;
- si ricorda che, nei casi in cui è indispensabile ed indifferibile accedere ai dati trattati dall'incaricato ed agli strumenti informatici in dotazione allo stesso, sia per le esigenze produttive sia per la sicurezza ed operatività dello stesso sistema informatico (ad esempio nei casi di prolungata assenza od impedimento dell'incaricato), il titolare potrà accedere ai dati e agli strumenti elettronici mediante intervento dell'amministratore di rete il quale è chiamato a modificare direttamente la parola chiave consentendo l'accesso ai dati, dandone tempestivamente conoscenza all'incaricato indisponibile quale possessore della credenziale;
- all'incaricato è fatto tassativo divieto di installare e utilizzare programmi per elaboratore non espressamente autorizzati dal Titolare in quanto potrebbero diffondere in modo fraudolento i dati personali conservati negli archivi elettronici;
- tutti gli strumenti informatici e telematici messi a disposizione costituiscono degli strumenti di lavoro da utilizzare esclusivamente per l'esecuzione delle mansioni affidate.

#### **7. Trattamento di dati personali senza l'ausilio di strumenti elettronici**

Nel caso di accesso e trattamento di dati personali su supporto di tipo cartaceo ubicati presso il proprio ufficio l'incaricato è tenuto a custodirli con diligenza, a non disperderli e a riporli negli appositi contenitori dopo l'uso.

Nel caso in cui tale documentazione contenga anche dati sensibili o giudiziari, l'incaricato può accedere agli archivi solo se preventivamente autorizzato.



L'incaricato potrà prelevare i documenti dagli archivi esclusivamente per effettuare operazioni di trattamento al medesimo consentite provvedendo al contempo alla loro diligente custodia.

L'incaricato, nel trattare documenti contenenti dati sensibili o giudiziari, è tenuto a custodirli fino alla restituzione in modo da evitare l'accesso agli stessi dati a persone prive di autorizzazione.

I documenti o copia degli stessi non possono, senza specifica autorizzazione, essere portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati in via generale dal Titolare.

L'incaricato deve inoltre controllare che i documenti, composti da numerose pagine o più raccoglitori, siano sempre completi, verificando che sia il numero dei fogli che l'integrità del contenuto, rispetto a quanto presente, all'atto del prelievo dal luogo sicuro.

Ci si deve in particolare accertare che un visitatore o terzo (addeito alla manutenzione, addetto alle pulizie, collega non autorizzato) possa entrare in ufficio anche non invitato o per cause accidentali, non possa venire a conoscenza dei contenuti dei documenti.

Si deve limitare al minimo assoluto il numero di fotocopie effettuate.

Eventuali fotocopie non riuscite bene debbono essere distrutte in un apposito distruggitore, se disponibile, oppure devono essere strappate in pezzi talmente piccoli, da non consentire in alcun modo la ricostruzione del contenuto, che deve essere comunque illeggibile.

È tassativamente proibito utilizzare le fotocopie non riuscite o stampe di computer, contenenti dati personali, come carta per appunti.

Quando i documenti devono essere trasportati all'esterno del luogo di lavoro, l'incaricato deve sempre custodire la cartella o la borsa, nella quale i documenti sono contenuti; deve inoltre evitare che sia possibile esaminare, da parte di un soggetto terzo non autorizzato, anche solo la copertina del documento in questione.

Durante il trasporto, la cartella non deve essere mai lasciata incustodita e preferibilmente deve essere tenuta chiusa a chiave o devono essere azionate le serrature a combinazione di presenti sulla cartella o valigia.

È tassativamente proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il corrispondente sia un incaricato, il cui profilo di autorizzazione sia tale da potere trattare i dati in questione.

## 8. Utilizzo di internet, e-mail e fax

Durante l'orario di lavoro sulla postazione assegnata è consentito utilizzare esclusivamente la mail istituzionale.

Non è consentito l'uso di social, se non quelli istituzionali per i quali si è ricevuto l'incarico.

La navigazione in internet deve avvenire esclusivamente sui siti istituzionali per lo svolgimento delle proprie mansioni lavorative.

## 9. Regole di condotta ex D.Lgs 231/2001

E' fatto divieto di:

1. falsificare documenti informatici pertinenti all'attività dell'Ente;
2. utilizzare le credenziali di accesso al sistema destinate ad altre persone;
3. installare programmi provenienti dall'esterno della rete scolastica senza l'autorizzazione del Titolare;
4. utilizzare le unità di rete nonché tutti i sistemi informatici (ivi compresi porte usb o notebook o altri PC portatili) per scopi diversi dalle mansioni lavorative individuali;
5. utilizzare i supporti magnetici (cd, dischetti, cassetta, cartucce) per finalità differenti rispetto a quelle previste dal Titolare;
6. caricare e scaricare (upload e/o download) files e/o programmi software, anche gratuiti, se non per esigenze strettamente lavorative e fatti salvi comunque i casi di esplicita autorizzazione;
7. effettuare ogni genere di transazione finanziaria salvo i casi direttamente autorizzati e con il rispetto delle normali procedure per gli acquisti;
8. partecipare a forum non autorizzati, utilizzare chat (esclusi gli strumenti autorizzati), utilizzare bacheche elettroniche o effettuare la registrazione in guest books anche utilizzando pseudonimi (o nicknames) e, più in generale, utilizzare qualunque utilizzo di servizi internet, attuali o futuri, non strettamente inerenti l'attività dell'ente;
9. lasciare i pc ed altri dispositivi elettronici incustoditi;
10. accedere a sistemi informatici altrui abusivamente, ovvero senza autorizzazione.



**LA DIRIGENTE SCOLASTICA**  
**Prof.ssa Anna Maria CIOFFI**

