ISTITUTO TECNICO INDUSTRIALE STATALE "GALILEO GALILEI"
52100 AREZZO Via Dino Menci, 1 - C.F.: 80002160515 – C.M.: ARTF02000T
Tel. 05753131 – Fax 0575313206
Posta elettronica: artf02000t@istruzione.it; artf02000t@pec.istruzione.it
Sito Internet: http://www.itisarezzo.edu.it

# ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI

Nello svolgimento delle funzioni, che comportano un trattamento di dati personali, il Personale Scolastico deve attenersi alle istruzioni contenute nel presente documento.

In attuazione del **principio di «liceità, correttezza e trasparenza»:**
- le operazioni di raccolta, registrazione, elaborazione di dati ed in generale, le operazioni di trattamento tutte, devono essere finalizzate esclusivamente all'inserimento o arricchimento degli archivi/banche dati della Scuola, nell'osservanza delle tecniche e metodologie in atto;
- la comunicazione o eventualmente la diffusione o il trasferimento all'esterno dei dati personali devono essere fatte esclusivamente a soggetti autorizzati a riceverli legittimamente, per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute dal Titolare del trattamento.

In attuazione del **principio di «minimizzazione dei dati»,** devono essere trattati esclusivamente i dati personali che si rivelino necessari rispetto alle finalità per le quali il dipendente è preposto.

In attuazione del **principio di «limitazione della finalità»,** il trattamento deve essere conforme alle finalità istituzionali del Titolare e limitato esclusivamente a dette finalità.

In attuazione del **principio di «esattezza»**, il Personale Scolastico ha l'obbligo di assicurare l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati personali, ed ha l'obbligo di verificare la pertinenza, la completezza e non eccedenza rispetto alle finalità per le quali i dati sono stati raccolti, e successivamente trattati.

In attuazione del **principio di «limitazione della conservazione»**, il Personale Scolastico deve:
- 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;
- esercitare la dovuta diligenza affinché non vengano conservati, nella Scuola, dati personali non necessari o divenuti ormai superflui;
- alla conclusione del trattamento, deve assicurarsi che i documenti contenenti i dati di cui agli articoli 9 e 10 del GDPR vengano conservati in contenitori/armadi muniti di serratura od in ambienti ad accesso selezionato e vigilato, fatte salve le norme in materia di archiviazione amministrativa.

In attuazione del **principio di «integrità e riservatezza»**, il Personale Scolastico deve:
- garantire un'adeguata sicurezza dei dati personali, compresa la protezione, dando diligente ed integrale attuazione alle misure logistiche, tecniche informatiche, organizzative,

procedurali definite dal Titolare, trattando i dati stessi con la massima riservatezza ai fini di impedire trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.
In particolare:

- riporre in archivio, al termine del periodo di trattamento, i supporti ed i documenti, ancorché non definitivi, contenenti i dati personali;
- non fornire dati personali per telefono, qualora non si abbia certezza sull'identità del destinatario;
- evitare di inviare, per e-mail, documenti in chiaro contenenti dati personali (i documenti vanno inviati senza alcun esplicito riferimento all'Interessato).

In attuazione del **principio di «trasparenza»**, il Personale Scolastico deve:
- accertarsi dell'identità dell'Interessato, prima di fornire informazioni circa i dati personali od il trattamento effettuato;
- fornire all'Interessato (o verificare che siano state fornite) tutte le informazioni di cui agli articoli 13 e 14 del GDPR e le comunicazioni di cui agli articoli da 15 a 22 ed all'articolo 34 del GDPR, relative al trattamento utilizzando apposita modulistica o indicando il link di pubblicazione sul sito della scuola.
- agevolare l'esercizio dei diritti dell'Interessato ai sensi degli articoli da 15 a 22 del GDPR.

Le stesse istruzioni e prescrizioni cogenti sono obbligatorie anche per il trattamento di dati personali realizzato, interamente o parzialmente, con strumenti elettronici, contenuti in archivi/banche dati o destinati a figurarvi.

In particolare, per tali trattamenti la persona fisica Autorizzata al trattamento ha l'obbligo di utilizzo e gestione attenendosi alle seguenti istruzioni:

**A) Strumenti elettronici in generale**

- I personal computer fissi e portatili ed i programmi per elaboratore su di essi installati sono uno strumento di lavoro e contengono dati riservati e informazioni personali di terzi ai sensi della normativa sulla protezione dei dati personali: vanno, pertanto, utilizzati e conservati, insieme ai relativi documenti esplicativi, con diligenza e cura, attenendosi alle prescrizioni fornite dal Titolare e nel rispetto delle indicazioni da questo fornite.
- In generale, tutti i dispositivi elettronici sono forniti per lo svolgimento della sua attività lavorativa, nell'ambito delle mansioni a questo affidate. L'uso per fini personali è da considerare, pertanto, eccezionale e limitato a comunicazioni occasionali e di breve durata, ad esclusione dei dispositivi per i quali è esplicitamente regolamentato l'uso per fini personali.
- Le impostazioni dei personal computer e dei relativi programmi, per elaboratore installati, sono predisposti dagli addetti informatici incaricati sulla base di criteri e profili decisi dal Titolare, in funzione della qualifica del dipendente, delle mansioni cui questo è adibito, nonché delle decisioni e della politica di utilizzo di tali strumenti stabilite dalla Scuola. Il dipendente non può modificarle autonomamente; può ottenere cambiamenti nelle impostazioni solo previa autorizzazione.
- Assicurarsi, in caso di sostituzione del computer utilizzato, che siano effettuate le

necessarie operazioni di formattazione o distruzione dei supporti di memorizzazione dei dati.
- Rivolgersi tempestivamente, per difficoltà o questione inerente alla sicurezza, al Dirigente scolastico o al DPO.
- Per finalità di assistenza, manutenzione ed aggiornamento e previo consenso esplicito del dipendente stesso, l'Amministratore di Sistema o soggetti appositamente incaricati allo svolgimento di tale attività potranno accedere da remoto al personal computer del dipendente attraverso un apposito programma "software".
- Il dipendente è tenuto ad osservare le medesime precauzioni e cautele, ove queste siano applicabili e pertinenti rispetto allo specifico strumento utilizzato, in relazione a tutti i dispositivi elettronici di cui fa uso, tra cui ad esempio fax, fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari, pen-drive e supporti di memoria;

La Scuola ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati.

**B) Predisposizione di atti e documenti da pubblicare sul sito web istituzionale**

Il Personale Scolastico preposto alla pubblicazione di atti e documenti sul sito istituzionale della Scuola, prima di pubblicare qualunque informazione sul sito web istituzionale non espressamente richiesto dal Titolare, dal Dirigente o da un suo diretto collaboratore, deve adottare opportuni accorgimenti, tra cui:

- individuare se esiste un presupposto di legge o di regolamento che legittima la diffusione del documento o del dato personale;
- verificare, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni;

Fermi restando i casi di divieto previsti dalla legge, i dipendenti non possono divulgare o diffondere, per ragioni estranee al loro rapporto di lavoro con l'Amministrazione e in difformità alle disposizioni di cui al decreto legislativo 13 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità.

**C) Password e username (credenziali di autenticazione informatica)**

Il Personale Scolastico deve utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui ed astenendosi dall'accedere a servizi telematici non consentiti.
Le credenziali di autenticazione informatica sono individuali e non possono essere condivise.

In particolare:
- è vietato comunicare a terzi gli esiti delle proprie interrogazioni delle banche dati;
- i codici identificativi, le password e le smart card saranno disattivate nel caso in cui i dipendenti cessino il loro rapporto di lavoro, oltre che nei casi espressamente e tassativamente previsti dalla normativa (in tali casi il dipendente è tenuto a restituirle agli uffici a ciò preposti);

- la password che la persona fisica designata e autorizzata al trattamento imposta:
  - deve essere sufficientemente lunga e complessa e deve contemplare l'utilizzo di caratteri maiuscoli e speciali e numeri (almeno 8 caratteri);
  - non deve essere riconducibile alla persona;
  - deve essere cambiata almeno ogni 3/6 mesi;
  - non deve essere rivelata o fatta digitare al personale di assistenza tecnica o a terzi;
  - non deve essere rivelata o comunicata al telefono, via fax od altra modalità elettronica.

**D) Assenza od impossibilità temporanea o protratta nel tempo**

- Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività del Titolare sia necessario accedere ad informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare a un altro dipendente a sua scelta ("fiduciario") il compito di verificare il contenuto di messaggi e inoltrare - quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere redatto apposito verbale e informato il dipendente interessato alla prima occasione utile.
- In caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività dell'ufficio sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, ed il dipendente non abbia delegato un suo fiduciario, secondo quanto sopra specificato, il Dirigente scolastico può richiedere con apposita e motivata richiesta all'Amministratore del Sistema di accedere alla postazione e/o alla casella di posta elettronica del dipendente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari. Contestualmente, il Dirigente scolastico deve informare il dipendente dell'avvenuto accesso appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale.

**E) Log-out**

- In caso di allontanamento anche temporaneo dalla postazione di lavoro (personal computer fisso o portatile), il dipendente non deve lasciare il sistema operativo aperto con la propria password e/o smart card inserita. Al fine di evitare che persone estranee effettuino accessi non consentiti, il dipendente deve attivare il salvaschermo con password o deve bloccare il computer e togliere la smart card dall'apposito alloggiamento.

**F) Utilizzo della rete internet e relativi servizi - Cloud storage**

- non è consentito navigare in siti web non attinenti allo svolgimento delle mansioni assegnate;
- non è consentita la registrazione a servizi on-line, a titolo o per interesse personale;
- 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 e con il rispetto delle normali procedure di acquisto;
- non è permessa la partecipazione, per motivi non professionali, a servizi di forum, l'utilizzo di chat-line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);
- il dipendente si impegna a circoscrivere gli ambiti di circolazione e di trattamento dei dati personali (es. memorizzazione, archiviazione e conservazione dei dati in cloud) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 (Paese terzo giudicato adeguato dalla Commissione Europea, BCR di gruppo, clausole contrattuali modello, consenso degli interessati, etc.).

**G) Posta elettronica**

La casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell'ambito dell'attività lavorativa.
L'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può, in alcun modo, compromettere la sicurezza o la reputazione della Scuola.
L'utilizzo di caselle di posta elettronica personali è di norma evitato per attività o comunicazioni afferenti il servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale.
I dipendenti non sono autorizzati ad utilizzare gli indirizzi di posta elettronica istituzionali assegnati per le comunicazioni personali.
Le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta nel rispetto della normativa vigente.
È vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.
Il dipendente è responsabile del contenuto dei messaggi inviati.
La posta elettronica diretta all'esterno della rete della Scuola può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti contenenti dati personali di cui agli articoli 9 e 10 del GDPR.
Non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale della Scuola per la partecipazione a dibattiti esterni, forum o mailing list per attività non inerenti alla didattica o non istituzionali.
Qualora si verifichino anomalie nell'invio e ricezione dei messaggi di posta elettronica sarà cura del dipendente informare prontamente l'Amministratore di sistema o il Dirigente scolastico.

**H) Software, applicazioni e servizi esterni**

Sui PC forniti dalla scuola per l'esercizio delle funzioni previste, occorre attenersi alle seguenti indicazioni.
- Al fine di evitare il pericolo di introdurre virus informatici nonché di alterare la stabilità

delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dall'Amministratore di sistema o figura analoga ovvero dal Dirigente scolastico.
- Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.
- Non è consentito modificare le configurazioni impostate sui PC.
- Non è consentito configurare gli strumenti per la gestione della posta elettronica per la gestione di account privati. Non è inoltre consentito utilizzare detti strumenti per la ricezione, visualizzazione ed invio di messaggi a titolo personale.
- Il Titolare si riserva la facoltà di procedere alla rimozione di ogni file od applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti od installati in violazione delle presenti istruzioni.
- Tutti i software caricati sul sistema operativo ed in particolare i software necessari per la protezione dello stesso o della rete internet (quali antivirus o firewall) non possono essere disinstallati o in nessun modo manomessi, (salvo quando questo sia richiesto dall'amministratore di sistema per compiere attività di manutenzione o aggiornamento).

**I) Reti di comunicazione**

- Nel caso di trattamento di dati personali effettuato mediante elaboratori non accessibili da altri elaboratori (cioè mediante computer stand alone) è necessario utilizzare la parola chiave (password) fornita per l'accesso al singolo PC.
- Nel caso di trattamento di dati personali effettuato mediante elaboratori accessibili da altri elaboratori, solo in rete locale, o mediante una rete di telecomunicazioni disponibili al pubblico, è necessario: utilizzare la parola chiave (password) fornita per l'accesso ai dati, oltre che servirsi del codice identificativo personale per l'utilizzazione dell'elaboratore.
- Le unità di rete o lo spazio all'interno del Registro elettronico sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque "file" che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
- Al fine di garantire la disponibilità dei documenti di lavoro assicurandone il backup periodico, si dovrà procedere al loro salvataggio nell'apposita area di rete individuale o di gruppo a ciò dedicata e disponibile sui sistemi server del Titolare.
- Non collegare dispositivi che consentano un accesso, non controllabile, ad apparati della rete del Titolare.
- Non è consentito accedere a servizi non autorizzati di peer to peer; non è altresì consentito condividere in qualunque forma e modalità materiale elettronico tutelato dalle normative sul diritto d'autore (software, file audio, film, etc.).

**J) Utilizzo dei mezzi di informazione e dei social media**

- Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla Scuola di appartenenza.
- In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che

possa nuocere al prestigio, al decoro o all'immagine della Scuola.
- Al fine di garantirne i necessari profili di riservatezza, le comunicazioni, afferenti direttamente o indirettamente il servizio, non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.

**K) Supporti esterni di memorizzazione**

La persona fisica designata e autorizzata al trattamento, ha l'obbligo di:
- proteggere i dati personali archiviati su supporti esterni con le stesse misure di sicurezza previste per i supporti cartacei;
- verificare che i contenitori degli archivi/banche dati (armadi, cassettiere, computer, etc.) vengano chiusi a chiave e/o protetti da password in tutti i casi di allontanamento dalla postazione di lavoro;
- evitare che i dati estratti dagli archivi/banche dati possano divenire oggetto di trattamento illecito;
- evitare di asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la previa autorizzazione;
- procedere alla cancellazione dei supporti esterni contenenti dati personali, prima che i medesimi siano riutilizzati. Se ciò non è possibile, essi devono esser distrutti;
- verificare l'assenza di virus nei supporti utilizzati.

Arezzo, 4 novembre 2024

**IL DIRIGENTE SCOLASTICO**
Prof. Luca Decembri
(Documento informatico firmato digitalmente
ai sensi del testo unico D.P.R. 28/12/2000 n. 445,
del D.Lgs. 07/03/2005 n. 82 e norme collegate)