UNIONE EUROPEA

REGIONE SICILIANA

ISTITUTO D'ISTRUZIONE SECONDARIA SUPERIORE "ARCHIMEDE"
Via G. Bonfiglio, 44 - 92022 Cammarata (AG.)
Tel. 0922-909401 Fax 0922-901268 - C.F. e P. IVA: 93074180840
Sito web: www.iiss-archimede.edu.it–e-mail: agis026008@istruzione.it – pec: agis026008@pec.istruzione.it

*Sede centrale II.SS "Archimede"- Cammarata (AGIS026008) *** Sez. Associata I.T.I. "Archimede" - Cammarata (AGTF02601R)Sez. Associata I.P.S.I.A. "Archimede"- Cammarata (AGRI02601X) *** Sez. Associata I.P.S.I.A . " Archimede" - Casteltermini (AGRI026021) Corso serale Sez. Associata I.P.S.I.A . " Archimede" - Casteltermini (AGRI026508)*

II.SS. " ARCHIMEDE " - CAMMARATA
Prot. 0001889 del 28/03/2020
07 (Uscita)

LINEE GUIDA PER IL TRATTAMENTO E LA PROTEZIONE DEI DATI PERSONALI INCARICATI (*) DEL TRATTAMENTO IN REGIME DI SMART WORKING

(*) Rif. Regolamento: persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare.

ASSISTENTI AMMINISTRATIVI DELL'ISTITUTO

PREMESSA

La situazione d'emergenza che stiamo vivendo è tale da non permettere il normale svolgimento delle attività lavorative presso la sede della Scuola, in attuazione delle misure di contenimento alla diffusione del COVID – 19, per un periodo che si spera essere breve ma che, in potenza, potrebbe anche estendersi oltre i termini attualmente indicati qualora l'emergenza sanitaria non accennasse ad un suo ridimensionamento.

Le presenti Linee Guida contengono la descrizione delle misure operative che gli assistenti amministrativi sono chiamati ad adottare per garantire la sicurezza dei dati personali dei soggetti interessati durante lo svolgimento delle attività lavorative in regime di Smart Working

Tale nuova modalità lavorativa comporta nuove criticità; la maggiore è data dall'uso di dispositivi personali per accedere ai Sistemi dell'Istituto, ivi incluse le connessioni di rete (ADSL, WiFi, ecc.) dove magari non si sono modificati i parametri standard (incluse le password amministrative, disponibili con una semplice ricerca su Google).

Molto spesso a casa, utilizzando dispositivi personali e non forniti dall'azienda, si tende a trascurare le misure di sicurezza, non si adottano (o non in maniera adeguata) sistemi antivirus/antimalaware, e si sottovalutano i piccoli rischi normalmente connessi alla navigazione in rete e accettati con ingenuità (accesso a siti pericolosi, download, ecc.).

In tale scenario, è quindi alta la possibilità che i computer abbiano malware attivi, o che qualcuno possa intercettare le nostre comunicazioni senza particolari difficoltà: uno scenario seriamente pericoloso se si accede, in questo modo, ai sistemi della Scuola.

Definizioni

Costituisce trattamento qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la

modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati.

Misure operative generiche

Nello svolgimento delle sue mansioni, l'incaricato dovrà:

- accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
- trattare i dati personali in modo lecito e secondo correttezza;
- raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli solo per operazioni di trattamento compatibili con le finalità connesse all'attività svolta;
- verificare che i dati siano esatti e, se necessario, aggiornarli;
- verificare che i dati siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- conservare i dati in 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;
- non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
- informare prontamente il Titolare o il Responsabile per la Protezioni dei Dati dell'Istituto (RPD), di seguito indicato, di ogni circostanza idonea a determinare pericolo di dispersione o utilizzo non autorizzato dei dati stessi;
- non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Titolare e, comunque, senza avere la certezza della loro identità;
- non lasciare a disposizione di estranei documenti o supporti di memorizzazione (cd, dvd, pen drive) che contengono dati personali o sensibili;
- accertarsi della distruzione di documenti inutilizzati contenenti dati personali o sensibili;
- non abbandonare la postazione di lavoro, senza aver provveduto a custodire in luogo sicuro i documenti contenenti dati personali;
- collaborare con il Responsabile per la Protezione dei Dati dell'Istituto, indicato nel seguito del documento, per aspetti specifici relativi ad ogni nuova attività che comporti il trattamento dei dati personali.

Misure operative specifiche all'utilizzo di tecnologie informatiche

- Scegliere per i diversi software gestionali (Personale, Didattica, eccetera) una password che sia composta da otto caratteri e non facilmente intuibile, evitando che contenga riferimenti alla propria persona (es. proprio nome o di congiunti, date di nascita, ecc.).
- Curare la conservazione della propria password dei software gestionali e non comunicarla per alcun motivo a soggetti terzi.
- Cambiare periodicamente (almeno una volta ogni tre mesi) la propria password dei software gestionali.
- Adottare le stesse cautele di cui sopra per le password di qualsiasi altra piattaforma software ad uso personale e potenzialmente interessata al Trattamento di Dati Personali (mail, account per piattaforme terze, eccetera).

- Effettuare il logoff dai software gestionali e, laddove presenti, da sistemi di autenticazione di rete al termine di ogni sessione di lavoro.

- Spegnere correttamente il computer al termine di ogni sessione di lavoro al fine di agevolare, se utilizzati, l'azione di software specifici di congelamento delle configurazioni degli stessi.

- Non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password.

- Nella comunicazione multimediale con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall'Istituto; è fatto divieto utilizzare social network quali Facebook o altri.

- Nell'utilizzo della posta elettronica non aprire documenti di cui non sia certa la provenienza e controllare accuratamente l'indirizzo dei destinatari prima di inviare email contenenti in allegato o nel corpo del messaggio dati personali.

- Nell'esercizio delle proprie mansioni utilizzare esclusivamente le apparecchiature informatiche fornite dalla scuola, presenti negli uffici di segreteria: ufficio segreteria del personale, ufficio di segreteria didattica, ufficio affari generali, eccetera), in quanto tali attrezzature sono regolarmente sottoposte a rigide misure di sicurezza e in linea con le misure minime di sicurezza ICT emanate dall'AGID. (Tale misura è derogata in ipotesi di Smart Working).

Disposizioni specifiche per il lavoro da casa con uso dei propri dispositivi personali

- Aggiornare il sistema operativo in uso
- Installare o verificare il sistema antivirus ed effettuare un'accurata scansione preventiva.
- Se possibile installare un sistema di gestione remota del PC, con il quale i colleghi tecnici possano monitorare e gestire eventuali problemi (come ad esempio piattaforme Kaseya, Solarwind, ManageEngine).
- Privilegiare l'uso delle applicazioni in cloud nello svolgimento delle attività lavorative.
- Privilegiare se possibile accessi remoti "terminalizzati" (ad esempio con strumenti Microsoft o Citri). In questo assetto sul computer remoto viene eseguita una sessione che mostra una elaborazione che viene svolta in totale sicurezza sui sistemi aziendali, evitando una interazione diretta tra il sistema remoto ed il sistema Informativo aziendale.
- Avvalersi di una connessione VPN ovvero quel canale di comunicazione "sicuro" tra il dispositivo remoto e l'azienda, attraverso il quale si accede direttamente agli applicativi ed ai dati aziendali.
- Aumentare il grado di complessità delle password utilizzate, e di forzarne il cambiamento molto più frequentemente di quanto si faccia normalmente (possibilmente anche una volta alla settimana).
- In caso di "uso promiscuo" del personal computer o del tablet (per esempio con altri componenti il nucleo familiare) l'assistente amministrativo avrà cura di attivare un account riservato per le attività lavorative
-

Divieti

E' esplicitamente vietato:

- effettuare copie su supporti magnetici o trasmissioni non autorizzate di dati oggetto del trattamento o di dati inerenti le mansioni del proprio profilo professionale.

- diffondere e/o divulgare notizie inerenti le proprie mansioni o quelle di altre unità di personale al di fuori degli uffici amministrativi (atti, documenti in originale o in copia fotostatica, password, login, ecc.).

- effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate, di stampe, tabulati,elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

- sottrarre, cancellare, distruggere, senza esplicita autorizzazione, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.

Qualunque violazione delle modalità sopra indicate dà luogo a precise responsabilità, ai sensi delle normative vigenti.

Dati del Titolare e del Responsabile per la Protezione dei Dati (RPD

Il titolare del trattamento è l'Istituzione Scolastica, rappresentata dal Dirigente Scolastico

Il Responsabile per la Protezione dei Dati, nel seguito indicato sinteticamente come RPD, è:

- Idnet Management Srls . nella persona del Dott Alfredo Giangrande

  con sede legale in via Palermo, Via Siracusa 34, 90141 (PA) Partita IVA 06291800826,

  email: giangrande.alfredo@gmail.com

  PEC personale: idinet@legalmail.it

La presente viene pubblicata sul sito della scuola nella sezione privacy **www.iiss-archimede.edu.it/school/privacy/** ed inviata al DSGA e agli assistenti amministrativi.

Il Dirigente Scolastico
(Prof. Antonino Pardi)
Firma autografa sostituita a mezzo stampa,
ai sensi dell'art.3, comma 2, del D.Lgs n.39/93