DISCIPLINARE E MANUALE OPERATIVO PRIVACY

Azienda/Organizzazione	**ISTITUTO COMPRENSIVO STATALE FALCOMATA' - ARCHI**

DIRIGENTE SCOLASTICO	CORRADO SERAFINA

SEDE	**Sede** **ISTITUTO COMPRENSIVO STATALE FALCOMATA' - ARCHI** **Via Montello 7,** **89125 - Reggio Calabria**

Prot. 7343 del 06/10/2021

Pur non essendo obbligatorio, il presente manuale intende rappresentare una guida per tutti collaboratori dell'organizzazione in materia di trattamento dei dati personali di persone fisiche.

DATI AZIENDA

RAGIONE SOCIALE	ISTITUTO COMPRENSIVO STATALE FALCOMATA' – ARCHI
SEDE LEGALE/OPERATIVA	VIA MONTELLO 7 – REGGIO CALABRIA
COD. FISCALE	92081760800
PEC	Rcic80500x@pec.istruzione.it
EMAIL	Rcic80500x@istruzione.it
TELEFONO	096548679
SITO INTERNET	http://www.icfalcomatarchi.edu.it/
ATTIVITA' SVOLTA	ISTRUZIONE PUBBLICA
CODICE ATECO	
RAPPRESENTANTE LEGALE *COGNOME E NOME*	CORRADO SERAFINA
RAPPRESENTANTE LEGALE *C.F.*	OMISSIS
RAPPRESENTANTE LEGALE *CONTATTI*	Serafina.corrado2@gmail.com

1. DEFINIZIONI

General Data Protection Regulation (GDPR)
Il Regolamento generale per la protezione dei dati personali n. 2016/679 è la normativa europea in materia di protezione dei dati personali di persone fisiche. Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, è entrato in vigore il 24 maggio 2016 ma la sua attuazione è avvenuta a distanza di due anni, a partire dal 25 maggio 2018.
Trattandosi di un regolamento non necessita di recepimento da parte degli Stati dell'Unione per cui è attuato allo stesso modo in tutti gli Stati dell'Unione. Il suo scopo è, infatti, la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea.

Trattamento
Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, 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 di dati, anche se non registrati in una banca di dati.

Dato personale
Qualsiasi informazione concernente una persona fisica identificata o identificabile (art. 4 GDPR), anche indirettamente, oppure informazioni (es. codice fiscale, impronta digitale, traffico telefonico, immagine, voce) riguardanti una persona la cui identità può comunque essere accertata mediante informazioni supplementari.

Dati particolari
I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Profilazione
Per profilazione si intende l'insieme delle attività di raccolta ed elaborazione dei dati inerenti agli utenti di un servizio, al fine di suddividerli in gruppi a seconda del loro comportamento. In ambito commerciale, la profilazione dell'utente è il mezzo che consente la fornitura di servizi personalizzati oppure l'invio di pubblicità comportamentale.

Pubblicità comportamentale
La pubblicità comportamentale è una tecnica basata sul tracciamento (tracking) delle attività online degli utenti, al fine di costruire dei profili degli utenti con lo scopo di offrire loro pubblicità più rilevante per gli utenti stessi, e quindi più efficace.

Titolare
Il Titolare del trattamento (data controller) è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali" (art. 4. par. 1, n. 7 GDPR).

Responsabile del trattamento
Il responsabile del trattamento è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare (art. 4, par. 1, n. 8 GDPR).

Sub responsabile

Il responsabile del trattamento può nominare responsabili di secondo livello a meno che non sia vietato dalle istruzioni del titolare. È comunque il responsabile principale a rispondere di fronte al titolare del trattamento dell'operato dei sub-responsabili. Al sub-responsabile devono essere fornite le istruzioni e deve operare nel rispetto degli obblighi imposti al responsabile del trattamento.

Persona autorizzata
Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato
La persona fisica a cui si riferiscono i dati personali.

Banca dati
Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Misure di sicurezza
Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che assicurano un livello di protezione adeguato dei dati personali.

Strumenti elettronici
Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Autenticazione informatica
L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Credenziali di autenticazione
I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

Parola chiave
Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

Profilo di autorizzazione
L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Sistema di autorizzazione
L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

2. RUOLI, COMPITI E NOMINA DEI SOGGETTI

2.1 Titolare del Trattamento

Il **Titolare del trattamento è** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Il **Titolare del trattamento**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Responsabili del trattamento dati** che assicurino e garantiscano che vengano adottate le misure di sicurezza. Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile del trattamento dei dati** ne assumerà tutte le responsabilità e funzioni.

2.2 Responsabile del Trattamento dati

2.2.1 Compiti delle persone autorizzate al trattamento dei dati personali

Il responsabile del trattamento (data processor) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR).
Si tratta di un soggetto, distinto dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.
Il titolare del trattamento risponde della gestione effettuata dal responsabile, dovendo ricorrere a responsabili che presentino garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che soddisfino i requisiti del Regolamento (Considerando 81 GDPR), e che le sue decisioni siano conformi alle leggi. Compito specifico del titolare è, infatti, quello di valutare il rischio del trattamento che pone in essere tramite i responsabili. Il titolare deve sempre poter sindacare le decisioni dei responsabili.
Il responsabile ha obblighi di trasparenza, occorre, infatti contrattualizzare il rapporto tra titolare e responsabile specificando gli obblighi ed i limiti del trattamento dati. Il responsabile riceverà, tramite atto giuridico (cioè per iscritto), tutte le istruzioni in merito ai trattamenti operati per conto del titolare, alle quali dovrà attenersi. Inoltre il responsabile del trattamento dovrà mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'articolo 28 del Regolamento, e dovrà tenere il registro dei trattamenti svolti (ex art. 30, paragrafo 2, GDPR).
Il responsabile ha, poi, l'obbligo di garantire la sicurezza dei dati adottando tutte le misure di sicurezza adeguate al rischio (art. 32 GDPR), tra le quali anche le misure di attuazione dei principi di privacy by design e by default, garantendo la riservatezza dei dati, vincolando i dipendenti, informando il titolare delle violazioni avvenute ed occupandosi della cancellazione dei dati alla fine del trattamento.

2.2.2 Nomina del Responsabile del trattamento dei dati personali

La nomina di ciascun Responsabile del trattamento dei dati personali deve essere effettuata dal Titolare del trattamento con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.

2.3 Persona autorizzata al trattamento dei dati personali

2.3.1 Compiti delle persone autorizzate al trattamento dei dati personali

Gli **Incaricati del trattamento** sono le persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali dal **Responsabile del trattamento**.

In particolare gli incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:
A tal fine, vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal titolare/responsabile;
- in ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:
    - divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del titolare/responsabile;
    - l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
    - la fase di raccolta del consenso dovrà essere preceduta dalla informativa ed il consenso al trattamento degli interessati rilasciato in forma scritta;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le proprie credenziali di autenticazione devono essere riservate;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- qualsiasi altra informazione può essere fornita dal Titolare che provvede anche alla formazione.

2.3.2 Nomina delle persone autorizzate al trattamento dei dati personali

La nomina di ciascuna **Persona autorizzata al trattamento dei dati personali** deve essere effettuata dal **Titolare** o dal **Responsabile del trattamento** con una **lettera di incarico** in cui sono specificati i compiti che gli sono stati affidati che deve essere controfirmata dall'interessato per presa visione.

3. NOMINE

Di seguito, è riportato l'organigramma con le funzioni nominate per la gestione della protezione del trattamento dati personali:

SEDE

ISTITUTO COMPRENSIVO STATALE FALCOMATA' - ARCHI

Via Montello 7,

89125 - Reggio Calabria

Titolare del trattamento:	**CORRADO SERAFINA (DIRIGENTE)**	
Responsabili interno del trattamento:	CANNIZZARO GIOVANNI FILIPPO (DSGA)	
Responsabili esterni del trattamento:		
Persone autorizzate:		
DPO:	**ROMEO DOMENICO**	
Medico competente:		
Amministratore di sistema:		
Custode Password:		
Nomina generica:		

4. ATTIVITÀ DI TRATTAMENTO DATI PERSONALI

Il presente capitolo riporta l'elenco delle attività di trattamento dati personali e per ognuno sono indicate le seguenti informazioni:

- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

VALUTAZIONE DEI RISCHI - METODOLOGIA UTILIZZATA

Per ogni attività di trattamento è stata eseguita la valutazione dei possibili scenari di rischio. Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili

2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ **LR** ≤ 3)*
Medio - basso	*(4 ≤ **LR** ≤ 6)*
Rilevante	*(8 ≤ **LR** ≤ 12)*
Alto	*(15 ≤ **LR** ≤ 25)*

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

Elenco attività sottoposte a DPIA

a. Attività didattiche

Struttura	SEDE LEGALE ED OPERATIVA

Personale coinvolto	
Titolare del trattamento	CORRADO SERAFINA (DIRIGENTE)
Persone autorizzate	CORRADO SERAFINA C.F. OMISSIS (DIRIGENTE) CANNIZZARO GIOVANNI FILIPPO, C.F. OMISSIS (DSGA) BAGNATO MARIA ANTONIETTA, C.F. OMISSIS (ASSISTENTE AMMINISTRATIVO) CUTRUPI FRANCESCA, C.F. OMISSIS (ASSISTENTE AMMINISTRATIVO) MARRA ERNESTA, C.F. OMISSIS (ASSISTENTE AMMINISTRATIVO) NAPOLI ADRIANA, C.F. OMISSIS (ASSISTENTE AMMINISTRATIVO) ZIRILLI CARMELA STEFANIA, C.F. OMISSIS (ASSISTENTE AMMINISTRATIVO) SETTIMIO SAVERIO MARIA ALBERTO, C.F. OMISSIS (ASSISTENTE TECNICO) TOSCANO CARMEN, C.F. OMISSIS (1° COLLABORATORE DEL DIRIGENTE SCOLASTICO) ARCONTE MARIA FILIPPA, C.F. OMISSIS (2° COLLABORATORE DEL DIRIGENTE SCOLASTICO) ALBANO ROSARIA CARMELA, C.F. OMISSIS (COORDINATORE DIDATTICO DI PLESSO) CAPPELLACCIO PATRIZIA, C.F. OMISSIS (COORDINATORE DIDATTICO DI PLESSO) MARRA ANTONIETTA ROSA, C.F. OMISSIS (COORDINATORE DIDATTICO DI PLESSO) LEOTTA FRANCESCA ELEONORA, C.F. OMISSIS (COORDINATORE DIDATTICO DI PLESSO) CALARCO MILENA, C.F. OMISSIS (COORDINATORE DIDATTICO DI PLESSO) PANSERA MARIA, C.F. OMISSIS (COORDINATORE DIDATTICO DI PLESSO) SORGONA' GEMMA LUCIA, C.F. OMISSIS (COORDINATORE DIDATTICO DI PLESSO)
Partners - Responsabili esterni	MUSOLINO GIUSEPPE, c.f. OMISSIS (Medico)

Processo di trattamento		
Descrizione	Attività didattiche	
Fonte dei dati personali	Forniti da terzi Raccolti direttamente	
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Consenso Contratto	
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Consenso Contratto Legge	
Finalità del trattamento	Adempimento di obblighi fiscali o contabili; Attività di consulenza; Contratto di assunzione; Gestione dei fornitori (contratti, ordini, arrivi, fatture); Gestione del personale; Gestione dell'utenza Igiene e sicurezza del lavoro; Informazione per via telematica; Newsletter; Relazioni con il pubblico; Pubblicità e promozione iniziative e di soggetti terzi (partner); Analisi del bisogno e progettazione servizi; Erogazione servizi e attività formative, sociali, ricreative, educative, socio-assistenziali; Progettazione educativa; Raccolta fondi; Iscrizione e aggiornamento dei dati utenti in software gestionale SIDI MIUR Adempimento di obblighi fiscali o contabili; Attività di consulenza; Contratto di assunzione;	
Tipo di dati personali	Dati personali: Codice fiscale ed altri numeri di identificazione personale (carte sanitarie); Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc. Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.); Dati relativi alla famiglia e a situazioni personali; Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare); Dati relativi all'attività economica e commerciale; Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae; Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro). Dati particolari: Sensibili (medici) e giudiziari (situazione individuale e familiare)	
Categorie di interessati	Aderenti ad associazioni politiche, religiose o sindacali; Agenti e Rappresentanti; Artigiani; Clienti ed utenti; Collaboratori; Commercianti;	Clienti ed utenti Agenti e Rappres Amministratori Appartenenti all' Collaboratori Consulenti e liber

	Condomini; Consulenti e liberi professionisti, anche in forma associata; Dipendenti; Enti; Istituti di credito e assicurativi Familiari dell'interessato; Fornitori; Imprenditori e piccoli imprenditori; Industrie; Lavoratori Autonomi; Personale pubblico dirigenziale e magistrati; PMI (Piccole e Medie Imprese); Potenziali clienti; Soci associati ed iscritti; Soggetti o organismi pubblici.	Dipendenti Enti Fornitori Lavoratori Autono Consulenti estern Familiari dell'inte Pazienti Membri di organis
Categorie di destinatari	ASL e Commissioni mediche Altre amministrazioni pubbliche; Autorità di vigilanza e controllo; Camere di commercio, industria, artigianato ed agricoltura; Clienti ed utenti; Consulenti e liberi professionisti anche in forma associata; Datore di lavoro; Enti locali; Istituti di credito e assicurativi Forze di polizia; Persone autorizzate; Enti previdenziali ed assistenziali; Interessati; Medico competente; Ordini e collegi professionali; Organizzazioni sindacali e patronati; Organismi paritetici in materia di lavoro; Rappresentante dei lavoratori per la sicurezza; Enti pubblici e privati in relazione ai rapporti di lavoro e di consulenza; Compagnie di assicurazione con cui l'Istituto abbia stipulato eventuali polizze; Agenzie di viaggio e/o strutture alberghiere e/o enti gestori degli accessi a musei, gallerie, monumenti, fiere, in occasione di visite guidate e viaggi di istruzione; Compagnie teatrali, compagnie circensi in occasioni di spettacoli e/o attività integrative che coinvolgano gli allievi e/o il personale della scuola; Scuole, enti e/o associazioni accreditati per la gestione di corsi di aggiornamento e formazione; Enti certificatori di competenze linguistiche o informatiche; Imprese, ditte o studi professionali in occasioni di stage o esperienze di alternanza scuola-lavoro	

Informativa	Si
Profilazione	SI: Bisogni del cliente, caratteristiche personali, emotive ed educative. Abitudini e dinamiche familiari, del singolo e del minore.
Dati particolari	SI: Sensibili e giudiziari. - Acquisizione in alcuni casi di dati medici, diagnosi, patologie, terapie. - Acquisizione dati giudiziari se necessari, riferiti alla situazione familiare del minore. (esempio provvedimenti di affidamento, separazione,….) - Acquisizione dati religiosi delle famiglie - Acquisizione dati sindacali dei dipendenti
Consenso minori	SI
Frequenza trattamento	Giornaliera
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	SI: dati dell'alunno per trasferimento in altra scuola estero e/o per stage alunni in altro paese)
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale Pacchetto Office Faldoni e Cartelle cartacee ed informatiche
Archiviazione	Stanza archivio con diniego di accesso al pubblico Armadio chiuso a chiave
Strutture informatiche di archiviazione	
Strutture informatiche di backup	
Archivio Informatico Scuola	Struttura interna : Server con Nas – Hard Disk Esterni
Sede di riferimento	ISTITUTO COMPRENSIVO STATALE FALCOMATA' – ARCHI Sede Via Montello 7, 89125 - Reggio Calabria
Frequenza di backup	1 giorni
Tempo di storicizzazione	30 giorni
Personale con diritti di accesso	CORRADO SERAFINA, C.F. OMISSIS (DIRIGENTE) CANNIZZARO GIOVANNI FILIPPO, C.F. OMISSIS (DSGA) BAGNATO MARIA ANTONIETTA, C.F. OMISSIS (ASSISTENTE AMMINISTRATIVO) CUTRUPI FRANCESCA, C.F. OMISSIS (ASSISTENTE AMMINISTRATIVO) MARRA ERNESTA, C.F. OMISSIS (ASSISTENTE AMMINISTRATIVO) NAPOLI ADRIANA, C.F. OMISSIS (ASSISTENTE AMMINISTRATIVO) ZIRILLI CARMELA STEFANIA, C.F. OMISSIS (ASSISTENTE AMMINISTRATIVO) SETTIMIO SAVERIO MARIA ALBERTO, C.F. OMISSIS (ASSISTENTE TECNICO)

	TOSCANO CARMEN, C.F. OMISSIS (1° COLLABORATORE DEL DIRIGENTE SCOLASTICO) ARCONTE MARIA FILIPPA, C.F. OMISSIS (2° COLLABORATORE DEL DIRIGENTE SCOLASTICO) ALBANO ROSARIA CARMELA, C.F. OMISSIS (COORDINATORE DIDATTICO DI PLESSO) CAPPELLACCIO PATRIZIA, C.F. OMISSIS (COORDINATORE DIDATTICO DI PLESSO) MARRA ANTONIETTA ROSA, C.F. OMISSIS (COORDINATORE DIDATTICO DI PLESSO) LEOTTA FRANCESCA ELEONORA, C.F. OMISSIS (COORDINATORE DIDATTICO DI PLESSO) CALARCO MILENA, C.F. OMISSIS (COORDINATORE DIDATTICO DI PLESSO) PANSERA MARIA, C.F. OMISSIS (COORDINATORE DIDATTICO DI PLESSO) SORGONA' GEMMA LUCIA, C.F. OMISSIS (COORDINATORE DIDATTICO DI PLESSO) MUSOLINO GIUSEPPE, c.f. OMISSIS (Medico)
Note	Personale con diritto di accesso: DOCENTI CON NOMINA DI INCARICO DI CUI SI ALLEGA ELENCO AL REGISTRO
Software utilizzati	SOFTWARE GESTIONALE – FILE EXCEL SERVER CLOUD CERTIFICATI UTILIZZATI: Axios Cloud – Sidi Miur

VALUTAZIONE DEL LIVELLO DI RISCHIO			
RISCHIO	**PROBABILITÀ**	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Accesso dati non autorizzato	Poco probabile	Gravissime	Rilevante
Distruzione non autorizzata	Poco probabile	Gravi	Rilevante
Divulgazione non autorizzata	Poco probabile	Gravissime	Rilevante

Modifica non autorizzata	Poco probabile	Gravissime	Rilevante
Perdita	Probabile	Gravi	Rilevante

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati - Dispositivi antincendio - E' applicata una gestione della password degli utenti - E' applicata una procedura per la gestione degli accessi - E' eseguita la DPIA - E' presenta una politica per la sicurezza e la protezione dei dati - Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati - Esistono procedure per l'individuazione del custode delle password - I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili - Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi - Le password sono costituite da almeno otto caratteri alfanumerici - Le password sono modificate al primo utilizzo - Le password sono modificate ogni 3 mesi - Le procedure sono riesaminate con cadenza predefinita - L'impianto elettrico è certificato ed a norma - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee - Registrazione e deregistrazione degli utenti - Sistemi di allarme e di sorveglianza anti-intrusione - Sono applicate regole per la gestione delle password. - Sono definiti i ruoli e le responsabilità - Sono definiti i termini di conservazione e le condizioni di impiego dei dati. - Sono gestiti i back up - Sono stabiliti programmi di formazione e sensibilizzazione - Sono utilizzati software antivirus e anti intrusione - Viene eseguita opportuna manutenzione - Viene eseguita una regolare formazione del personale

5. ASSET AZIENDALI

Gli asset sono tutti gli strumenti utilizzati dall'organizzazione per trattare e conservare i dati personali quali:

- server, computer, tablet, smartphone, sistemi di rilevazione presenze;
- programmi software sia installati su dispositivi aziendali che utilizzati in cloud;
- archivi relativi a database, cartelle condivise, ecc.

Di seguito la mappatura di tutti gli strumenti:

Denominazione	**Archivio informatico**
Tipo Struttura	Interna
Sede	ISTITUTO COMPRENSIVO STATALE FALCOMATA' – ARCHI Sede Via Montello 7, 89125 - Reggio Calabria
Personale con diritti di accesso	DSGA – AMMINISTRATIVI DELEGATI
Note	Server con Nas – Hard Disk Esterni
Software utilizzati	SOFTWARE GESTIONALE – FILE EXCEL

Denominazione	**AXIOS CLOUD - SIDI MIUR**
Tipo Struttura	Esterna
Azienda	AXIOS - MIUR
Personale con diritti di accesso	DSGA – AMMINISTRATIVI DELEGATI
Note	Software cloud
Software utilizzati	SERVER CLOUD CERTIFICATI UTILIZZATI: AXIOS CLOUD – SIDI MIUR

6. ISTRUZIONI OPERATIVE

6.1 ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI

INDICE

PREMESSA

L'utilizzo delle risorse informatiche e telematiche della nostra Azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. Istituto Comprensivo "Falcomatà Archi" ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

1. UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.

Il custode delle parole chiave riservate, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno previa autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Responsabile dei sistemi informatici* della Istituto Comprensivo "Falcomatà Archi" L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo

autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*.
Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.
Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del *Responsabile dei sistemi informatici aziendali*.
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Responsabile dei sistemi informatici aziendali* nel caso in cui vengano rilevati virus.

2. UTILIZZO DELLA RETE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il *Responsabile dei sistemi informatici aziendali* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

3. GESTIONE DELLE PASSWORD

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal *Responsabile dei sistemi informatici aziendali*.
È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al *Responsabile dei sistemi informatici aziendali. (n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al Responsabile; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'incaricato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presente regolamento)*
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
La password deve essere immediatamente sostituita, dandone comunicazione al *Responsabile dei sistemi informatici aziendali*, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne

immediata notizia alla Direzione o al *Responsabile dei sistemi informatici aziendali*.

4. UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati particolari (ex dati sensibili) e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati particolari (ex dati sensibili) e giudiziari devono essere custoditi in archivi chiusi a chiave.

5. UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli dal *Responsabile dei sistemi informatici aziendali* e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

6. USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata dall'Azienda all'utente, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per Istituto Comprensivo "Falcomatà Archi". deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).
Per la trasmissione di file all'interno di Istituto Comprensivo "Falcomatà Archi". è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al *Responsabile dei sistemi informatici aziendali*. Non si devono in alcun caso attivare gli allegati di tali messaggi.

7. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Responsabile dei sistemi informatici aziendali*.
È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

8. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI
È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

9. NON OSSERVANZA DELLA NORMATIVA AZIENDALE
Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

10. AGGIORNAMENTO E REVISIONE
Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.
Il presente Regolamento è soggetto a revisione con frequenza annuale.

6.3 ISTRUZIONI OPERATIVE DATA BREACH

L'art. 33 del **Regolamento Europeo 679/2016** (**GDPR**) e la normativa nazionale in vigore, impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**) entro 72 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR e della normativa nazionale in vigore.

Per **"Violazione di dati"** si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 p.12 del GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 p.5 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

E' importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

Si possono distinguere tre tipi di violazioni:

- violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
- violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
- violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.
-

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

- **Rischio assente**: la notifica al Garante non è obbligatoria.
- **Rischio presente**: è necessaria la notifica al Garante.
- **Rischio elevato**: In presenza di rischi "elevati", è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione.

6.4 ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO

INDICE

PREMESSA

Il presente documento contiene le istruzioni operative per gli Incaricati del trattamento dei dati personali dell'Azienda Istituto Comprensivo "Falcomatà Archi"., conformemente al Regolamento (Ue) 2016/679 (GDPR) ed alla normativa nazionale in vigore. I dipendenti, i collaboratori, i consulenti, i volontari ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativa ai dati, devono ispirarsi a un principio generale di diligenza e correttezza. Ogni utilizzo dei dati in possesso dell'Azienda diverso da finalità strettamente professionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine dell'Azienda.

1. DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR) e la normativa nazionale in vigore, si definisce:

- Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione

mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

2. ADEMPIMENTI

Ciascun incaricato del trattamento deve:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

3. MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI

Le principali operazioni degli incaricati del trattamento sono:

- identificazione dell'interessato:

al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;

- verifica del controllo dell'esattezza del dato e della corretta digitazione:

al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

- Norme logistiche per l'accesso fisico ai locali:

I locali, ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il trattamento di Dati Personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di Dati Personali.

- Rilevazione presenze

Ove possibile, si raccomanda di dotare le sedi dell'Azienda di un servizio di rilevazione delle presenze e di un servizio di reception / sorveglianza. In questo caso, ogni Incaricato è tenuto ad utilizzare sempre i sistemi di rilevazione presenze disponibili, allo scopo di segnalare la propria presenza e legittimare le attività in corso di svolgimento.

4. ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).
Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

b. Gestione strumenti elettronici (pc fissi e portatili)

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato.
Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario che:
• al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;
• Se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto deve chiudere la sessione di lavoro sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;
• Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:

- Non deve mai essere disattivato;
- Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
- Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;

• Quando si esegue la stampa di un documento contenente dati personali, in particolare su

una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.
Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:
• prima della riconsegna, rimuovere eventuali file ivi elaborati;
• quando il PC portatile è nei locali dell'Azienda, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…) utilizzando gli appositi cavi in acciaio dotati di lucchetto;
• quando il PC portatile è all'esterno dell'Azienda, evitare di lasciarlo incustodito;
• per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte;
• in caso di furto di un portatile è necessario avvertire tempestivamente il responsabile del Servizio Informatico, onde prevenire possibili intrusioni ai sistemi aziendali;
• in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;
• eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

c. Gestione username e password

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:
• tutela l'utilizzatore ed in generale l'Azienda da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
• tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;
• è necessario per gestire correttamente gli accessi a risorse condivise.
Ciascun incaricato deve scegliere le password in base ai seguenti criteri:
• devono essere lunghe almeno otto caratteri;
• non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;
• devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
• non deve essere uguali alle precedenti.
Per la corretta gestione della password è necessario:
• Almeno ogni 3 mesi è obbligatorio cambiare la password;
• Ogni password ricevuta va modificata al primo utilizzo;
• La password venga conservata in un luogo sicuro;
• Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;
• Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

d. Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico su mandato del Responsabile del trattamento per i Sistemi Elettronici. Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:
• Non utilizzare sul PC dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati;
• Non installare sistemi per connessione esterne (es : modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di

intrusioni e di attacchi dall'esterno;
• Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;
• Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.
Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Informatico, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

e. Gestione posta elettronica aziendale

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità della Azienda e in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.
Al fine di non compromettere la sicurezza dell'azienda e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:
• Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
• È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
• La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.
Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:
• l'indirizzo del destinatario sia stato correttamente digitato,
• l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
• nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;

f. Gestione del salvataggio dei dati

▪ Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.

▪ Per i dati ed i documenti che risiedono esclusivamente sul PC, ogni Incaricato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…). L'Incaricato deve verificare che i supporti informatici utilizzati per il backup, che normalmente sono dischi magnetici esterni, CD, DVD oppure flash disks (chiavette) siano funzionali e non corrotti.

g. Gestione dei supporti rimovibili

I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati. Tali operazioni vengono effettuate a cura del servizio Sistemi. Il trasferimento di file contenenti dati personali, dati

particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (ex dati sensibili)/giudiziari devono essere crittografati.

h. Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'Azienda è stato installato un software antivirus aziendale che si aggiorna automaticamente all'ultima versione disponibile.
L'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.
Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico.
Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

COMPITI SPECIFICI PERSONALE SCOLASTICO IC FALCOMATÀ ARCHI

1. Utilizzo della postazione di lavoro

1.1 All'utente viene messa a disposizione una stazione di lavoro predisposta e configurata dall'Ufficio Tecnico. Ogni utilizzo della stessa non inerente all'attività lavorativa è vietato in quanto potenzialmente idoneo a innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Gli strumenti della postazione di lavoro devono essere custoditi con cura evitando ogni possibile forma di danneggiamento.
La strumentazione messa a disposizione è configurata in modo tale da ridurre al minimo l'utilizzazione di dati personali e di dati identificativi e da escluderne il trattamento qualora le finalità perseguite nei singoli casi possano essere realizzate mediante dati anonimi o modalità che permettano di identificare l'interessato solo in caso di necessità.
1.2 L'infrastruttura tecnologica è a tutti gli effetti un bene dell'IC Falcomatà Archi.
1.3 La strumentazione data in affidamento all'utente permette l'accesso alla piattaforma istituzionale Geuite ed al dominio Axios solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 2 del presente Regolamento.
1.4 Il Titolare del trattamento rende noto che il personale incaricato dell'Ufficio Tecnico, dell'IC Falcomatà Archi, è stato autorizzato a compiere interventi nel sistema informatico e informative diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware etc.). Detti interventi potranno anche comportare l'accesso, in caso di effettiva necessità, ai dati trattati da ciascuno, nonché la verifica riguardante i siti internet acceduti dagli utenti abilitati alla navigazione esterna.
Il personale incaricato dell'Ufficio Tecnico ha la facoltà di collegarsi e visualizzare in remoto il desktop e cartelle delle singole postazioni al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, etc..
L'intervento viene effettuato esclusivamente su richiesta dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico.
In quest'ultimo caso, sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso all'utente.
1.5 Salvo preventiva autorizzazione del personale dell'Ufficio Tecnico, non è consentito l'uso di programmi diversi da quelli ufficialmente installati per conto dell'IC Falcomatá Archi, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno,

sussistendo, infatti, il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone lo stesso Istituto a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software, la quale impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.
1.6 Salvo preventiva autorizzazione del personale dell'Ufficio Tecnico, non è consentito all'utente di modificare le caratteristiche impostate e le configurazioni apportate, né di procedere ad installare dispositivi (come ad esempio masterizzatori, modem, etc.).
1.7 Lasciare la postazione con il login effettuato, espone l'utente ad accessi di soggetti terzi e possibili indebite modifiche ad atti pubblici (es registro elettronico) sanzionabili penalmente ed ascrivibili all'utente stesso.

2. Gestione ed assegnazione delle credenziali di autenticazione

2.1 Le credenziali di autenticazione per l'accesso al dominio Axios vengono assegnate dal personale dell'Ufficio Tecnico.
2.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), associato ad una parola chiave 1° accesso (password). La password dovrà essere custodita dall'incaricato con la massima diligenza e non divulgata.
La parola chiave, deve essere composta da almeno otto caratteri alfanumerici, una lettera maiuscola, non deve contenere riferimenti agevolmente riconducibili all'incaricato, inoltre deve essere diversa dalle ultime tre inserite.
2.3 È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, ogni 100 gg quando il sistema ne notifica la scadenza.

3. Navigazione Internet

3.1 Gli utenti possono utilizzare la strumentazione informatica connessa ad Internet anche per la navigazione in rete, ove la funzione lo preveda e sotto la propria responsabilità. La navigazione deve comunque avvenire nel rispetto della legge, dell'ordine pubblico, del buon costume e delle norme di prudenza e cautela atte ad evitare problemi di sicurezza al sistema informativo dell'Istituto.
3.2 A titolo puramente esemplificativo, l'utente non potrà utilizzare Internet per:
a) l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e/o musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale dell'Ufficio Tecnico);
b) l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Dirigenza o eventualmente dal DSGA e comunque nel rispetto delle normali procedure di acquisto;
c) ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
d) accessi a connessioni anonime o connessioni cifrate che, non permettono l'identificazione dell'indirizzo di navigazione, o comunque a connessioni che esulano quelle autorizzate dal sistema.
e) Al termine di ogni sessione assicurarsi di effettuare correttamente il logout. Non salvare le password su dispositivi sprovvisti di account personale. E' sconsigliabile farlo in ogni caso.
f) Utilizzare browsers in modalità anonima riduce I rischi di tracciamento.

4. Controlli

Gli eventuali controlli, compiuti dal personale incaricato dell'Ufficio Tecnico (anche esterno) per la verifica di condotte illecite o anomalie di sistema, ai sensi del precedente punto 1.5, potranno avvenire attraverso sistemi (quali ad esempio firewall che consentono, oltreché la creazione di black list, blocchi e filtri, anche il monitoraggio della navigazione web effettuata da ciascun utente), e anche mediante verifica dei file log. Il trattamento sarà svolto in forma automatizzata e manuale, con modalità e strumenti volti a garantire la massima sicurezza e riservatezza, ad opera di soggetti appositamente incaricati a tali attività.
Sarà facoltà del Dirigente, solo in caso di effettiva necessità, tramite il personale Tecnico o tramite addetti esterni alla manutenzione dei sistemi informatici, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici lavorativi e ai documenti ivi contenuti.
Ai sensi e per gli effetti di cui all'art. 4 comma 3, L. n. 300/1970, l'Istituto informa che il personale incaricato del servizio Tecnico, ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC, ovvero dei Notebook, come anche di visualizzare le singole cartelle contenute sui predetti dispositivi e i relativi file, assieme alla cronologia della navigazione internet ed i messaggi di posta elettronica.
Il controllo con i sistemi sopra descritti non è continuativo ed è effettuato solo da personale appositamente incaricato per il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Istituto. Sarà in ogni caso applicato il principio di liceità, proporzionalità e limitazione del trattamento.

5. Social Media Policy

IC Falcomatà Archi riconosce i benefici apportati dai social media, tuttavia, pur dichiarandosi favorevole al loro utilizzo, ritiene che l'utilizzo di questi canali di comunicazione possa presentare alcuni rischi.
Per tale motivo, con il presente Regolamento, si forniscono alcune indicazioni per un utilizzo responsabile degli stessi.
a) è vietato l'utilizzo dei social network di natura personale e non lavorativa, durante l'orario scolastico.
b) non è consentita la pubblicazione di contenuti o materiali: coperti da riservatezza, offensivi, illegali, vessatori, diffamanti, minacciosi, volgari, osceni, che ledano diritti di terzi e/o che incoraggino condotte contrarie alle vigenti normative, ai codici di condotta o simili.

6. Protezione antivirus

6.1 Il sistema informatico del IC Falcomatà Archi è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico scolastico mediante virus o mediante ogni altro software aggressivo.
6.2 Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto al personale dell'Ufficio Tecnico.
6.3 Ogni dispositivo di provenienza esterna all'Istituto (inclusi smartphone) viene verificato dal programma antivirus ad ogni accesso alla rete scolastica.

7. Utilizzo di telefoni fissi, Smartphone, Mobile Device ed equiparati, fax e fotocopiatrici

7.1 Il telefono fisso affidato all'utente è uno strumento di lavoro. Salvo esplicita autorizzazione, ne viene concesso l'uso esclusivamente ai fini dello svolgimento dell'attività lavorativa; non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività scolastica stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza.
7.2 Qualora venisse assegnato un Mobile Device scolastico all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al Mobile Device si applicano le medesime regole: in particolare, (salvo esplicita autorizzazione) è vietato inviare o ricevere SMS e/o MMS o l'uso di chat e social media di natura personale o comunque non pertinenti allo svolgimento dell'attività lavorativa.
7.3 È vietato l'utilizzo dei dispositivi scolastici per fini personali, tanto per spedire quanto per ricevere.
7.4 È vietato l'utilizzo delle fotocopiatrici scolastiche per fini personali.
7.5 Gli eventuali controlli, compiuti dal personale incaricato ai sensi del precedente punto 1.5 potranno avvenire mediante sistemi tecnologici e/o fatturazione del traffico telefonico e/o dati, in grado di verificare in particolare il chiamante, i tempi di conversazione e il numero chiamato.

8. Sistemi tecnologici e controlli

8.1 Il Dirigente Scolastico, considerato il divieto di utilizzo di strumenti tecnologici preordinati al controllo dell'attività lavorativa del dipendente, garantisce che tali strumenti saranno installati, se del caso, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro, per la tutela del patrimonio scolastico, previa idonea informativa all'interessato.
8.2 Controllo difensivo: in presenza di seri indizi, il personale incaricato potrà effettuare, attraverso i predetti sistemi tecnologici, controlli rivolti ad accertare condotte illecite dell'utente anche mediante verifica dei file log presenti sulla strumentazione informatica, qualora, con dette modalità, non si pregiudichi la sicurezza del sistema e del trattamento dati;

i. ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi. I documenti di questo tipo contenenti dati particolari (ex dati sensibili) o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.
Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari (ex dati sensibili) e/o giudiziari, il rispetto di queste norme è obbligatorio.

a) distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

b) Misure di sicurezza

Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:
• la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;
• la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un tritadocumenti.

c) Prescrizioni per gli incaricati

L'Incaricato deve attenersi alle seguenti prescrizioni:
• in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
• la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
• l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
• i supporti devono essere archiviati in ambiente ad accesso controllato;
• i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
• il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
• cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
• l'accesso fuori orario lavorativo a documenti contenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
• la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
• ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il

volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
• quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati 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 particolari (ex dati sensibili) o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.
• è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

ii. ADDETTI ALLA MANUTENZIONE

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:
• Effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
• gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione dell'Amministratore di sistema;
• gestire i profili di autorizzazione degli incaricati al trattamento dei dati, su specifiche impartite dai responsabili di funzione/BU, su indicazione dell'Amministratore di sistema;
• provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili ovvero della Direzione Risorse Umane e su indicazione dell'Amministratore di sistema;
• custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali;
L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.
A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:
• Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.
• Nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.
• Per effettuare operazioni di manutenzione sui database aziendali che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.

• Devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;
• E' necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.
• Tutti i dati personali contenuti nei data base devono essere protetti da password;
• Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:
o in presenza dell'incaricato, far digitare la password dall'incaricato stesso evitando di venirne a conoscenza;
o in assenza dell'incaricato rivolgersi alla persona individuata dall'incaricato quale proprio fiduciario il quale provvederà all'inserimento della password.
• Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;
• L'amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione;
• Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;
• l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;
• E'assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla società, se non previa espressa comunicazione scritta;
• Nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza

iii. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

iv. NON OSSERVANZA DELLA NORMATIVA ISTITUTO

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

v. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Dirigente dell'Istituto.
Il presente Regolamento è soggetto a revisione con frequenza annuale.