



**Ministero dell'Istruzione, dell'Università e della Ricerca**  
**Ufficio Scolastico Regionale per il Lazio**  
**Istituto Statale D'Istruzione Superiore**  
**“VIA DELL'IMMACOLATA 47”**

Via dell'Immacolata n.47 – 00053 Civitavecchia (RM)  
Tel 06121124295 – Fax 0766500028

e-mail: [rmis10100r@istruzione.it](mailto:rmis10100r@istruzione.it) pec:[rmis10100r@pec.istruzione.it](mailto:rmis10100r@pec.istruzione.it)

**AUTORIZZAZIONI ADDETTI – DOCENTI**

Civitavecchia, 7/10/2022

Al personale docente in servizio a T.I. ed a T.D.  
Amministrazione Trasparente – sez. altri contenuti  
Sito web

Oggetto: **Misure finalizzate a dare attuazione alle disposizioni del Regolamento Europeo n.2016/679 e del D.lgs. n.196/03 “Codice in materia di protezione dei dati personali” e ss. mm. e ii. – Autorizzazioni Adetti al trattamento dei dati personali a.s. 2022-2023**

Premesso che:

- L'Istituto d'Istruzione Superiore “Via dell'Immacolata 47” – Via dell'Immacolata 47 - 00053 Civitavecchia (RM), rappresentato dal Dirigente Scolastico Prof. Roberto Ciminelli è titolare del trattamento dei dati personali di alunni, genitori, personale dipendente, fornitori, e qualunque altro soggetto che abbia rapporti con l'Istituto medesimo e che a questo conferisca, volontariamente o per obbligo, propri dati personali;
- Il personale in epigrafe, in servizio presso questo Istituto, per l'espletamento delle funzioni di docente, ha necessità di venire a conoscenza e di trattare dati personali, fermi restando gli obblighi e le responsabilità civili e penali;
- L'attività di trattamento è disciplinata dal Regolamento UE 2016/679 (di seguito Regolamento), dal D.lgs.196/03 come modificato dal D.lgs.101/18 (di seguito Codice) e dalle norme di settore,
- Per effetto del Regolamento il titolare del trattamento ha l'obbligo di adottare specifiche misure organizzative e di impartire istruzioni a tutti coloro che sono stati autorizzati al trattamento dei dati personali (artt.5,24,29,32);
- le Linee guida dell'Autorità Garante all'applicazione del Regolamento chiariscono che le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del Regolamento e che pertanto i titolari ed i responsabili del trattamento possono mantenere in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento;
- l'autorizzazione dell'addetto non implica l'attribuzione di funzioni ulteriori rispetto a quelle già assegnate, ma consente di trattare i dati, di cui si viene a conoscenza nell'esercizio dei compiti di docente, essendone stati autorizzati e avendo ricevuto le istruzioni sulle modalità cui attenersi nel trattamento;

Tutto ciò premesso,

l'Istituto d'Istruzione Superiore “Via dell'Immacolata 47” – Via dell'Immacolata 47- 00053 Civitavecchia (RM), rappresentato dal Dirigente Scolastico Prof. Roberto Ciminelli, autorizza le SS.LL. al trattamento dei dati personali detenuti da questa istituzione scolastica, come individuati negli allegati A (Ambito del trattamento consentito) e B (banche dati oggetto di trattamento).

Il trattamento dei dati personali consentito alle SS.LL. è strettamente limitato a quanto necessario ed indispensabile all'adempimento delle proprie mansioni, osservando inderogabilmente le norme di legge, i regolamenti interni, circolari, ordini di servizio, il manuale sulla sicurezza ad uso degli autorizzati al trattamento dei dati, alle istruzioni comunque impartite dal titolare del trattamento e dei suoi delegati. Le SS.LL. sono altresì tenute a seguire i corsi di formazione in materia di disciplina della protezione dei dati.

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto sono dovuti in base al vigente CCNL. Nel caso di inadempimento si applicheranno le sanzioni disciplinari previste dal vigente CCNL.

La presente autorizzazione ha efficacia fino alla risoluzione del rapporto di lavoro per qualsiasi causa oppure fino a modifica o revoca da parte del titolare del trattamento.

A titolo di documentazione amministrativa si chiede di firmare per ricevuta la seguente comunicazione.

Il Titolare del trattamento  
Istituto d'Istruzione Superiore "Via dell'Immacolata 47

(firma del Dirigente Scolastico)

.....

Per ricevuta:

I sottoscritti, di cui all'elenco allegato, dichiarano di aver ricevuto la presente autorizzazione al trattamento dei dati personali, corredata dagli Allegati A, B e C e si impegnano a seguirne e rispettarne tutte le specifiche istruzioni, attentamente esaminate e comprese. I sottoscritti si impegnano, altresì, a rispettare il divieto di comunicazione e diffusione dei dati trattati nel corso del presente incarico, anche per il tempo successivo alla sua cessazione, senza limiti temporali.

**Allegare foglio firma docenti.**

**Allegato A - Ambito di trattamento consentito**

Nella qualità di docenti dell'Istituzione scolastica, le SS.LL. necessariamente partecipano a trattamenti di dati personali, riguardanti le operazioni specifiche svolte nell'area di attività nella quale sono impegnate e nell'ambito delle loro competenze professionali. Pertanto il trattamento dei dati personali, con riferimento alle operazioni di: raccolta, registrazione, organizzazione, conservazione, modifica, consultazione, comunicazione, diffusione, raffronto, cancellazione, può riguardare le seguenti attività:

1. attività didattica e partecipazione agli organi collegiali;
2. valutazione alunni;
3. tenuta documenti e registri di attestazione delle valutazioni e di documentazione inerente alla vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia quali ad esempio richieste, istanze e corrispondenza con le famiglie;
4. rapporti con famiglie ed alunni, anche in situazione di disabilità e/o di disagio psico-sociale che possono consistere nella ricezione di certificati medici relativi allo stato di salute, e nello scambio di informazioni contenute in: documenti di vario tipo riguardanti gli alunni disabili, documentazione clinica per assunzione farmaci, documentazione clinica di intolleranze, documentazione clinica H, DSA e BES, limitatamente alle operazioni di trattamento strettamente indispensabili;
5. raccolta dei contributi economici e/o tasse scolastiche,
6. adempimenti connessi all'organizzazione delle visite guidate ed ai viaggi d'istruzione;
7. adempimenti connessi alla realizzazione dei profetti e delle attività previsti nel PTOF, comprese le attività di alternanza scuola /lavoro e/o di orientamento in ingresso ed in uscita;
8. conoscenza delle informazioni relative alle professioni religiose;
9. eventuali adempimenti connessi alla gestione amministrativa degli alunni e del personale (es. registrazione presenze, attestazioni inerenti allo stato del personale, ecc.).

**Allegato B - Banche Dati**

Le SS.LL. sono autorizzate all'accesso e al trattamento dei dati personali, compresi quelli appartenenti a particolari categorie (ai sensi dell'art.9 del Regolamento UE) e relativi a condanne e reati (ai sensi dell'art.10 del Regolamento), degli alunni e delle rispettive famiglie, relativi alle classi loro assegnate e/o che partecipano a progetti o attività anche integrative e complementari cui il docente sia coinvolto per la realizzazione del PTOF, con i quali l'Istituzione Scolastica entra in relazione per i suoi fini istituzionali, nella misura e nei limiti stabiliti dal Regolamento, dal Codice e dal Regolamento recante "l'identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione" (D.M. n.305 del 07.12.06 ). I dati personali trattati dai docenti sono contenuti sia in archivi cartacei, che in archivi elettronici e digitali, e possono riguardare: il registro di classe, il registro personale, i registri dei verbali dei consigli, la documentazione relativa alla programmazione didattica, i documenti di valutazione, la documentazione su disabilità - disturbi specifici dell'apprendimento (DSA) - bisogni educativi speciali (BES), le certificazioni mediche degli studenti, la corrispondenza con le famiglie, le immagini trattate nell'ambito della realizzazione di attività didattiche e progetti di carattere educativo formativo, secondo quanto indicato nel PTOF . In alcuni casi riguardanti le attività didattiche integrative e complementari per gli alunni, e gli incarichi organizzativi o funzionali alla realizzazione dell'offerta formativa, i dati personali trattati dai docenti sono anche quelli relativi a esperti e consulenti esterni.

**Allegato C - Istruzioni specifiche sul trattamento dei dati personali**

Nel precisare che gli indirizzi operativi sinora forniti risultano coerenti con finalità e metodi cui la suddetta normativa privacy (Regolamento UE n.2017/679, D.lgs. n. 196/03 e ss. mm. e ii. e Decreto legislativo 10 agosto 2018, n.101) riconosce legittimità, si intende con la presente indicare formalmente i principi cui le SS.LL. dovranno comunque continuare ad attenersi nel trattamento dei dati personali fornendo le seguenti istruzioni:

1. Il trattamento dei dati personali deve avvenire ai sensi della normativa privacy vigente, in modo lecito e secondo correttezza, e seguendo le direttive impartite dal titolare del trattamento;
2. il trattamento dei dati personali è consentito solo per lo svolgimento delle funzioni istituzionali della Scuola;
3. i soggetti autorizzati potranno raccogliere e registrare i dati personali esclusivamente per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
4. gli addetti autorizzati dovranno mantenere assoluto riserbo sui dati personali di cui verranno a conoscenza nell'esercizio delle loro attività;
5. l'obbligo di mantenere la dovuta riservatezza in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico ricoperto presso questa istituzione scolastica, deve permanere in ogni caso, anche quando sia venuto meno l'incarico stesso;
6. i soggetti autorizzati, nell'ambito delle proprie attribuzioni lavorative, cureranno l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati, verificando inoltre che questi ultimi siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali essi stessi sono stati raccolti e successivamente trattati;

7. gli addetti autorizzati avranno cura, secondo le comuni regole della prudenza e della diligenza, di trattare i dati stessi con la massima riservatezza e di impedire, per quanto possibile, che estranei non autorizzati prendano conoscenza dei dati che loro mantengano all'esclusivo fine lavorativo;
8. in ogni operazione di trattamento andrà garantita la massima riservatezza e custodia degli atti e dei documenti contenenti dati personali, che devono essere mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate ad accedervi a prenderne visione o ad effettuare qualsivoglia trattamento;
9. l'accesso agli archivi contenenti dati particolari (ex sensibili e giudiziari) è consentito solo alle persone autorizzate ed è soggetto a continuo controllo secondo le misure di sicurezza predisposte dall'Istituzione scolastica;
10. in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'addetto autorizzato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non autorizzati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento - a tal fine, tra l'altro, l'addetto autorizzato deve assicurarsi sistematicamente che, i contenitori degli archivi e banche dati (scrivanie, cassette, armadi, computer fissi, laptop, tablet, etc.) siano chiusi a chiave e/o protetti da password (nel caso in cui il trattamento venga effettuato con strumenti elettronici e sistemi ICT) e che i dati dagli stessi estratti non possano divenire oggetto di trattamento improprio;
11. i soggetti autorizzati potranno comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ad altri soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute dal titolare del trattamento;
12. è vietata qualsiasi forma di diffusione e comunicazione dei dati personali trattati che, essendo strettamente funzionale allo svolgimento dei compiti affidati, non sia stata appositamente autorizzata dal Titolare del trattamento;
13. le comunicazioni anche verbali e/o telefoniche agli interessati dovranno avvenire in forma riservata; se effettuate per scritto dovranno essere consegnate in contenitori chiusi;
14. in caso di trasmissione di documenti contenenti dati personali l'addetto autorizzato si dovrà assicurare dell'identità dell'interessato che li riceve o di chi è stato delegato al ritiro del documento in forma scritta;
15. in caso di comunicazioni elettroniche ad alunni, colleghi, genitori, personale della scuola o altri soggetti coinvolti per finalità istituzionali, queste (comunicazioni) vanno poste in essere seguendo le indicazioni fornite dall'Istituzione scolastica e avendo presente la necessaria riservatezza delle comunicazioni stesse e dei dati coinvolti;
16. al termine del trattamento gli addetti autorizzati dovranno assicurarsi che gli atti e i documenti contenenti dati appartenenti a particolari categorie e relativi a condanne e reati, vengano conservati in contenitori muniti di serratura o in ambienti ad accesso selezionato e vigilato, fino alla restituzione;
17. al termine del trattamento, eventuali fogli a stampa o compilati a mano che siano stati prodotti e/o utilizzati nella fase istruttoria o preparatoria, qualora contenenti dati personali, devono essere distrutti e resi illeggibili;
18. ai soggetti autorizzati non è consentito asportare supporti informatici o cartacei né copiare documenti, contenenti dati personali di terzi, senza la previa autorizzazione del titolare del trattamento;
19. eventuali supporti removibili utilizzati (es. chiavi USB, hard disk portatili, ecc.) su cui sono memorizzati dati personali vanno custoditi con cura e non devono essere messi a disposizione o lasciati al libero accesso di terzi non autorizzati;
20. supporti removibili contenenti dati particolari (ex sensibili e giudiziari), se non utilizzati, vanno distrutti o resi inutilizzabili mediante apposite tecniche di cancellazione sicura dei dati, di formattazione e di distruzione, effettuate da operatori specializzati;
21. gli autorizzati saranno tenuti a rispettare ed applicare le misure di sicurezza idonee a salvaguardare la riservatezza e l'integrità dei dati, adottate dall'Istituto ed indicate nelle "Linee Guida" per il trattamento dei dati personali.

Le stesse norme si applicano obbligatoriamente al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento manuale, di dati personali contenuti in un archivio o destinati a figurarvi, e si differenziano in base alle modalità di trattamento, ovvero se il trattamento dei dati possa essere effettuato con o senza strumenti informatici.

#### *Archivi cartacei di dati personali*

L'archivio cartaceo viene comunque gestito nel pieno rispetto delle idonee misure di sicurezza in relazione al tipo di documentazione in esso contenuta. Gli eventuali atti e documenti contenenti dati personali compresi nelle particolari categorie e relativi a vicende giudiziarie sono affidati ai soggetti autorizzati per lo svolgimento dei relativi compiti; i medesimi atti e documenti sono controllati e custoditi dagli autorizzati 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 di particolari categorie e/o giudiziari è controllato e consentito solo agli addetti espressamente autorizzati.

Gli archivi cartacei vengono gestiti secondo le seguenti modalità:

- possono accedere alle informazioni contenute nell'archivio cartaceo solo gli addetti autorizzati
- l'accesso alle informazioni è consentito limitatamente ai soli dati personali la cui conoscenza è strettamente necessaria per lo svolgimento dei compiti assegnati;
- tutti i documenti che contengono dati personali sono conservati in archivi ad accesso selezionato;
- i documenti contenenti dati personali non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali e, nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento;
- i faldoni contenenti i dati sono archiviati in una forma che non consenta l'identificazione dell'interessato a chi non autorizzato e comunque per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti e successivamente trattati;
- per tutto il periodo in cui i documenti che contengono dati personali sono al di fuori dei locali individuati per la loro conservazione, gli addetti autorizzati non dovranno lasciarli mai incustoditi, adottando ogni cautela affinché ogni persona non autorizzata non venga a conoscenza del contenuto;
- al termine dell'orario di lavoro tutti i documenti che contengono dati personali devono essere riportati nei locali individuati per la loro conservazione;
- per evitare il rischio di diffusione dei dati personali, l'utilizzo di copie fotostatiche deve essere limitato ai casi strettamente necessari ed autorizzati dal titolare ed è comunque vietato utilizzare copie fotostatiche di documenti che contengono dati personali all'esterno del luogo di lavoro.

#### *Gestione archivi digitali e documenti informatici contenenti dati personali*

- Utilizzo delle credenziali di autenticazione
  - L'accesso alle procedure informatiche che trattano dati personali è consentito solo agli Incaricati in possesso di "credenziali di autenticazione" che permettano il superamento di una procedura di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (user-id) associato ad una parola chiave riservata (password) e/o in un dispositivo di autenticazione o in una caratteristica biometrica
  - Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
  - Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato
  - Gli addetti devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle istruzioni contenute nelle linee guida (LG) e nel manuale operativo ad uso degli addetti autorizzati (IS02 – Istruzioni operative addetti)
- Protezione del PC in dotazione e dei dati
  - Tutti i PC devono essere dotati di password rispondenti alle policy interne
  - Tutti i PC devono essere dotati di software antivirus aggiornato costantemente e con la funzione "Monitor" attiva
  - Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa, dotati di licenza e forniti dalla Scuola
  - Sono vietati i software scaricati da Internet o acquisiti autonomamente
  - Per evitare accessi illeciti, deve essere sempre attivato il salva schermo con password
  - Sui PC devono essere installati, appena vengono resi disponibili (e comunque almeno annualmente), tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti
  - Deve essere effettuato, con cadenza almeno settimanale un salvataggio di back-up di eventuali dati personali salvati in locale, presenti sul proprio PC personale o non condivisi tramite il server della Scuola
  - I supporti di memoria utilizzati per il back-up devono essere trattati secondo le regole definite al punto "Archivi cartacei di dati personali"
  - I supporti rimovibili contenenti dati di particolari categorie e/o giudiziari se non utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri addetti, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
- Cancellazione dei dati dai PC

- I dati personali conservati sui PC devono essere cancellati in modo sicuro, con tecniche efficaci effettuate ad opera del personale tecnico specializzato, prima di destinare i PC ad usi diversi

#### *Come comportarsi in presenza di pubblico*

- Evitare l'accesso degli ospiti in luoghi in cui siano trattati dati personali di particolari categorie ed altre informazioni riservate
- Assicurare che vengano rispettate opportune distanze di cortesia qualora siano presenti più persone contemporaneamente nello stesso luogo
- Se è necessario allontanarsi dal luogo del trattamento in presenza di ospiti, riporre i documenti contenenti dati personali, non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento e attivare il salvaschermo del PC
- Non rivelare o fare digitare le password dal personale di assistenza tecnica
- Non rivelare a nessuno le password - nessuno è autorizzato a chiederle
- Segnalare qualsiasi anomalia o situazione di pericolo per i dati trattati al titolare

#### *Regole generali per le password*

Ciascun addetto Autorizzato è in possesso di diverse credenziali di autenticazione, costituite da username e password (autenticazione semplice), per accedere ai servizi informatici istituzionali o su web, che dovrà utilizzare e gestire attenendosi alle seguenti istruzioni. Le credenziali di autenticazione in generale consentono all'addetto autorizzato l'accesso ad un computer o ad una rete, esse sono individuali e pertanto non vanno mai condivise con altri utenti (anche se autorizzati) e devono essere custodite con cura e diligenza, evitando che possano essere sottratte o copiate in qualche modo. La password deve essere composta da almeno otto caratteri, anche se più aumenta il numero dei caratteri più la password diventa "robusta" (si suggerisce intorno ai 15 caratteri), non deve essere riconducibile alla propria persona o contenere parole di uso comune (facili da indovinare) e deve essere cambiata da ciascun autorizzato almeno ogni 3 mesi. Per evitare accessi illeciti, al termine di ciascun trattamento l'addetto autorizzato dovrà uscire dall'applicazione utilizzata assicurandosi di avere eseguito il logout.

#### *Registri on line*

Per quanto concerne il trattamento dei dati in registri elettronici, ciascun addetto autorizzato è in possesso di una password e di uno username, le quali costituiscono le Sue credenziali di autenticazione. L'uso delle credenziali per la verifica dell'identità degli addetti consente l'accesso di ciascun utente autorizzato solo alle informazioni strettamente pertinenti al proprio ruolo e relative agli alunni a lui affidati. La procedura che l'addetto autorizzato dovrà seguire per l'utilizzo del registro elettronico sarà la seguente: accedere all'applicazione; digitare lo username; digitare la password; accedere ai dati; una volta ultimato il trattamento uscire dall'applicazione assicurandosi di aver chiuso il proprio account prima di lasciare la postazione o il proprio dispositivo incustodito (logout). La password che verrà assegnata inizialmente dovrà essere modificata al primo utilizzo rispettando le regole generali sopra indicate. La propria password deve essere mantenuta assolutamente riservata e non può essere comunicata in nessun caso ad un'altra persona. In caso di smarrimento, l'addetto autorizzato dovrà informare immediatamente e per iscritto la Segreteria dell'Istituto che provvederà, in forma riservata, al rilascio di una nuova. In caso di malfunzionamenti e anomalie che impediscano l'utilizzo del Registro elettronico, l'addetto autorizzato dovrà avvertire immediatamente il Titolare del trattamento.

L'addetto autorizzato nello svolgimento della sua funzione docente sarà tenuto alla massima riservatezza in tutti i casi in cui potrà venire a conoscenza dei dati personali riguardanti gli studenti (assenze, ritardi, uscite, giustificazioni, voti, note disciplinari, ecc.) contenuti nel Registro elettronico. I dati del registro elettronico non possono essere inseriti, modificati o cancellati dalle persone non autorizzate. Il trattamento illecito dei dati viene sanzionato in modo severo dalle leggi vigenti.

Per accedere al registro elettronico l'addetto autorizzato potrà utilizzare gli strumenti informatici messi a disposizione dalla Scuola ed eventualmente altri dispositivi digitali personali, previa autorizzazione scritta di accesso alla rete dell'Istituto da parte del Dirigente scolastico. I PC ed i portatili in dotazione ai docenti per accedere il registro elettronico sono beni di proprietà della scuola e pertanto devono essere conservati con la massima cura.

#### *Posta elettronica ed internet*

- Gli strumenti digitali ufficiali per la condivisione dei materiali tra colleghi e con gli studenti sono gli account e le mail istituzionali e non account e indirizzi e-mail personali, che possono essere utilizzati solo in ambito non lavorativo per scopi personali;
- non è consentito utilizzare la posta elettronica istituzionale e le piattaforme dedicate alla didattica digitale integrata per motivi non attinenti allo svolgimento delle mansioni assegnate;
- non utilizzare la posta elettronica per comunicare informazioni riservate, dati personali anche sensibili senza l'autorizzazione del titolare e/o del responsabile e senza garantirne l'idonea protezione - la posta elettronica può usata per inviare messaggi contenenti dati appartenenti a particolari categorie ai sensi dell'art.9 del Regolamento UE 2016/679, solo previa crittografia;

- è sconsigliato l'invio di messaggi e-mail con allegati molto grandi verso molti utenti ovvero utilizzare lo strumento di posta elettronica in maniera non appropriata causando danni all'intero sistema (ad esempio l'invio di una e-mail a 100 utenti con un allegato di 20MB).
- fare attenzione ai messaggi di posta elettronica verificandone la provenienza in quanto, essi rappresentano uno dei metodi più subdoli per veicolare contenuti di virus, worm e frodi (anche senza necessità di allegati), malware anche in grado di cancellare i dati o di renderli indisponibili, in particolare non aprendo e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio un mittente o natura dell'oggetto poco chiari) e non cliccando su eventuali link inseriti nella missiva;
- accertarsi sempre che i destinatari siano autorizzati ad entrare in possesso dei dati oggetto della comunicazione;
- non rispondere ai messaggi di posta elettronica provenienti da indirizzi non noti;
- non comunicare la propria e-mail istituzionale a siti, che hanno scarsa attinenza con l'attività e verso i quali non si ha interesse e/o sui quali si nutre il minimo dubbio riguardo alla loro attendibilità;

Inoltre, nell'utilizzo degli strumenti in dotazione (apparecchiature informatiche e connessioni alla rete scolastica) adottare le seguenti misure:

- Accedere solo ai siti i cui contenuti siano correlati all'attività lavorativa - è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- durante la navigazione, prima di selezionare un link, fare attenzione a tutti i messaggi provenienti dal browser che richiedono l'apertura, l'installazione o il salvataggio di files.
- non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal titolare;
- non è consentito lo scarico di software gratuiti (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal titolare;
- non è permessa la partecipazione, per motivi non professionali a Forum, l'utilizzo di chat line, social network, ecc., anche utilizzando pseudonimi (o nickname);
- è severamente vietato aggirare le protezioni applicate ai sistemi informatici con software capace di farlo.