



ISTITUTO COMPRENSIVO CHIOGGIA 3

SCUOLA INFANZIA - SCUOLA PRIMARIA – SCUOLA SECONDARIA DI 1° GRADO

Cod. Min. VEIC85000R Cod. Fiscale 91020300272 Ambito Territoriale 19

Presidenza e Segreteria Via P.Togliatti, 831 C.a.p. 30015 CHIOGGIA – VE

Tel. 041400096 e-mail veic85000r@istruzione.it P.E.C. veic85000r@pec.istruzione.it

<https://www.chioggia3.it/>

Circolare n. 25

Chioggia, 19.09.2023

Ai DOCENTI

Agli Assistenti Amministrativi

Al D.S.G.A.

Oggetto: Nomina Incaricato al trattamento dei dati personali ai sensi dell'art. 30 D.Lgs. 196/2003 e dell'art. 4 Reg. UE n. 679/2016.

Si invia in allegato, al personale in indirizzo, la **nomina di incaricato al trattamento dei dati personali ai sensi dell'art. 30 D. Lgs. 196/2003 e dell'art. 4 Reg. UE n. 679/2016**, da prendere visione e restituire debitamente datato e sottoscritto, tramite e-mail entro e non oltre venerdì 22 settembre 2023.

Cordiali saluti.



Il Dirigente Scolastico
Prof.ssa Sandra Zennaro



ISTITUTO COMPRENSIVO CHIOGGIA 3

SCUOLA INFANZIA - SCUOLA PRIMARIA – SCUOLA SECONDARIA DI 1° GRADO

Cod. Min. VEIC85000R Cod. - Fiscale 91020300272

Presidenza e Segreteria Via P. Togliatti, 831 - c.a.p. 30015 CHIOGGIA – VE

Tel. 041/400096 - e-mail veic85000r@istruzione.it

P.E.C. veic85000r@pec.istruzione.it

Al docente

SEDE

Oggetto: **Nomina Incaricato al trattamento dei dati personali ai sensi dell'art. 30 D. Lgs. 196/2003 e dell'art. 4 Reg. UE n. 679/2016**

IL DIRIGENTE

- Visto il decreto legislativo n. 196/2003 (Codice in materia di protezione dei dati personali)
- Visto il Regolamento UE n. 679/2016 (G.D.P.R. General Data Protection Regulation)
- Preso atto che l'art. 4 comma 1 lett. h) del d.lgs. n. 196/2003 definisce "incaricati" le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- Preso atto che l'art. 4 n. 10) prevede la figura della "persona autorizzata al trattamento" dei dati personali;
- Premesso che il Garante ha statuito che "Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene opportuno che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento" [nota: <http://www.garanteprivacy.it/titolare-responsabile-incaricato-del-trattamento>]
- Preso atto che l'art. 30 del d. lgs. 196/2003 dispone che:

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.
2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito";

- Preso atto che l'art. 29 del Reg. UE 679/2016 dispone che:

"Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri";

- Preso atto che l'art. 32 comma 4 del Reg. UE 679/2016 dispone che:

“Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri”;

DESIGNA

Il docente

INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

in relazione alle operazioni di elaborazione di dati personali, su supporto cartaceo e/o elettronico, ai quali il docente ha accesso nell'espletamento delle funzioni e dei compiti assegnati nell'ambito del rapporto di lavoro con questa istituzione scolastica e disciplinati dalla normativa in vigore e dai contratti di settore. In particolare, **in qualità di Docente** è incaricato delle operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, modifica, connesse alle seguenti funzioni e attività svolte:

Alunni e genitori

- attività didattica e partecipazione agli organi collegiali;
- valutazione alunni;
- tenuta documenti e registri di attestazione dei voti e di documentazione della vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia quali ad esempio richieste, istanze e corrispondenza con le famiglie;
- in questo quadro: rapporti con famiglie e alunni in situazione di disagio psico-sociale; ricezione di certificati medici relativi allo stato di salute degli alunni, documentazione alunni disabili, documentazione mensa/intolleranze, documentazione DSA e BES, nei limiti sempre di quanto strettamente indispensabile;
- eventuali contributi e/o tasse scolastiche versati da alunni e genitori;
- adempimenti connessi alle visite guidate e ai viaggi d'istruzione;
- conoscenza di dati relativi a professioni di fede religiosa;
- eventuali adempimenti connessi al rapporto di pubblico impiego (quali, per es., registrazione presenze, attestazioni inerenti allo stato del personale).

Le operazioni sopra descritte vanno rigorosamente effettuate tenendo presenti le istruzioni operative che seguono:

1. il trattamento dei dati personali cui il docente è autorizzato ad accedere, deve avvenire secondo le modalità definite dalla normativa in vigore, in modo lecito e secondo correttezza e con l'osservanza - in particolare - delle prescrizioni di cui al Regolamento UE 2016/679 e al Dlgs 196/2003;
2. il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola;
3. i dati personali, oggetto dei trattamenti, devono essere esatti ed aggiornati, inoltre devono essere pertinenti, completi e non eccedenti le finalità per le quali vengono raccolti e trattati;
4. è vietata qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia strettamente funzionale allo svolgimento dei compiti affidati e autorizzata dal responsabile o dal titolare del trattamento. Si raccomanda particolare attenzione a tutela del diritto alla riservatezza degli interessati (persone fisiche a cui afferiscono i dati personali);
5. si ricorda che l'obbligo di mantenere la dovuta riservatezza in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, deve permanere in ogni caso, anche quando sia venuto meno l'incarico stesso;
6. i trattamenti andranno effettuati rispettando le misure di sicurezza predisposte nell'istituzione scolastica; in ogni operazione di trattamento andrà garantita la massima

- riservatezza e custodia degli atti e dei documenti contenenti dati personali che non andranno mai lasciati incustoditi o a disposizione di terzi non autorizzati ad accedervi, prendervi visione o ad effettuare qualsivoglia trattamento;
7. le eventuali credenziali di autenticazione (codice di accesso e parola chiave per accedere ai computer e ai servizi web) attribuite alle SS.LL sono personali e devono essere custodite con cura e diligenza; non possono essere messe a disposizione né rivelate a terzi; non possono essere lasciate incustodite, né in libera visione. In caso di smarrimento e/o furto, bisogna darne immediata notizia al responsabile (o, in caso di assenza del responsabile, al titolare) del trattamento dei dati;
 8. nel caso in cui per l'esercizio delle attività sopra descritte sia inevitabile l'uso di supporti rimovibili (quali ad esempio chiavi USB, CD-ROM, ecc), su cui sono memorizzati dati personali, essi vanno custoditi con cura, ne messi a disposizione o lasciati al libero accesso di persone non autorizzate;
 9. si ricorda inoltre che i supporti rimovibili contenenti dati sensibili e/o giudiziari se non utilizzati vanno distrutti o resi inutilizzabili;
 10. si ricorda inoltre che l'accesso agli archivi contenenti dati sensibili o giudiziari è permesso solo alle persone autorizzate e soggetto a continuo controllo secondo le regole definite dallo scrivente;
 11. durante i trattamenti i documenti contenenti dati personali vanno mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate;
 12. al termine del trattamento occorre custodire i documenti contenenti dati personali all'interno di archivi/cassetti/ armadi muniti di serratura;
 13. i documenti della scuola contenenti dati personali non possono uscire dalla sede scolastica, né copiati, se non dietro espressa autorizzazione del responsabile o dal titolare del trattamento;
 14. in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'incaricato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non incaricati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento;
 15. le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata; se effettuate per scritto dovranno essere consegnate in contenitori chiusi;
 16. all'atto della consegna di documenti contenenti dati personali l'incaricato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta
 17. 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.

La presente designazione ha validità permanente (per tutto il tempo in cui il docente rimarrà in servizio presso l'Istituto) e pertanto non sarà soggetta a rinnovo annuale.

Il Dirigente Scolastico
Prof.ssa Sandra ZENNARO

.....

Per ricevuta:

LINEE GUIDA IN MATERIA DI SICUREZZA PER I DOCENTI INCARICATI DEL TRATTAMENTO

Attenersi scrupolosamente alle seguenti indicazioni per garantire la sicurezza dei dati personali e, in particolare, dei dati sensibili e giudiziari:

- Certificati medici per esonero dalle lezioni pratiche di Educazione Fisica o limitazione dell'attività sono consultati e poi restituiti agli uffici di Segreteria.
- Certificati medici e altri documenti di natura sensibile e non, relativi a particolari interventi didattici (integrazione di alunni portatori di handicap), sono consultati e poi restituiti agli uffici di Segreteria.
- Gli elaborati degli studenti sono di norma custoditi in archivio sicuro e per il tempo stabilito. Nei casi contenessero dati sensibili, vengono consegnati in busta chiusa alla Segreteria per una conservazione a parte previa informazione al Dirigente Scolastico.
- Eventuali documenti rilevanti sono consegnati agli uffici di Segreteria.
- Non divulgare dati personali di alunni, personale, etc. senza espressa autorizzazione.
- custodire in apposito armadio nella stanza individuata come sala professori dell'edificio i seguenti documenti:
 - Registro personale (per i docenti che ne usufruiscono)
 - qualunque altro documento contenente dati personali o sensibili: nei documenti contenenti dati sensibili devono essere in via assoluta omessi i riferimenti che rendono identificabili i soggetti interessati
- seguire le istruzioni per l'uso del Registro elettronico
- riporre il Registro di classe, al termine delle attività didattiche giornaliere, nell'apposito armadio per la sua custodia
- seguire le istruzioni per l'accesso ai PC dei laboratori e alle LIM delle aule
- tutte le comunicazioni indirizzate agli uffici della sede centrale, ad altro personale della scuola e al Dirigente Scolastico debbono essere consegnate in busta chiusa al Responsabile di plesso o al Protocollo della sede centrale
- Non consentire l'accesso alle aree in cui sono conservati dati personali su supporto cartaceo a estranei e a soggetti non autorizzati;
- Non consentire l'accesso a estranei al fax e alla stampante che contengano documenti non ancora ritirati dal personale;
- Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;
- Provvedere personalmente alla distruzione quando è necessario eliminare documenti inutilizzati;
- Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte;
- Non lasciare incustoditi eventuali registri contenenti indirizzi e recapiti telefonici del personale e degli studenti e non annotarne il contenuto sui fogli di lavoro;
- Utilizzare immagini e registrazioni audio degli alunni solo per attività istituzionali, ogni uso diverso o per utilizzi che presuppongono la diffusione via web, supporti ecc. deve essere autorizzata.

Uso di PC e delle LIM del registro e dell'account d'Istituto

- non memorizzare file contenenti dati personali, come ad esempio tabelloni dei voti scaricati dal sistema informatizzato del registro e dello scrutinio, e/o sensibili nei PC delle aule, dei laboratori e della sala insegnanti
- non lasciare supporti di memoria informatici (chiavette USB, DVD, ecc.), cartelle o altri documenti contenenti dati personali e/o sensibili a disposizione di estranei
- non consentire nel modo più assoluto agli alunni l'accesso alla LIM e ai PC dei laboratori, se non in propria presenza, vigilando sugli allievi per un uso corretto degli strumenti
- per l'uso del Registro Elettronico e della Posta elettronica, scegliere una password con le seguenti caratteristiche:
 - originale
 - composta da almeno otto caratteri
 - che contenga almeno un numero una lettera e un carattere speciale
- che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili
- curare la conservazione della propria password ed evitare di comunicarla ad altri
- cambiare periodicamente (almeno una volta ogni tre mesi) la propria password
- modificare prontamente la password assegnata
- spegnere correttamente il computer al termine di ogni sessione di lavoro o, nel caso in cui debba essere utilizzato da altro utente, mettere in atto le apposite misure di sicurezza
- uscire dall'account prima di lasciare la postazione di lavoro promiscua, si consiglia di utilizzare il browser in modalità "navigazione anonima"
- comunicare tempestivamente qualunque anomalia riscontrata nel funzionamento del computer
- utilizzare le seguenti regole per la Posta elettronica e la condivisione dei documenti:
 - non aprire documenti di cui non sia certa la provenienza
 - non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
 - controllare accuratamente l'indirizzo del destinatario o l'account qualora sia necessario inviare/condividere documenti contenenti dati personali
 - nella comunicazione multimediale per fini istituzionali con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall'Istituto; è fatto divieto utilizzare social network quali Facebook o altri
 - Per l'attività didattica utilizzare le piattaforme informatiche approvate dall'Istituto

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



ISTITUTO COMPRENSIVO CHIOGGIA 3

SCUOLA INFANZIA - SCUOLA PRIMARIA – SCUOLA SECONDARIA DI 1° GRADO

Cod. Min. VEIC85000R Cod. - Fiscale 91020300272

Presidenza e Segreteria Via P. Togliatti, 831 - c.a.p. 30015 CHIOGGIA – VE

Tel. 041/400096 - e-mail veic85000r@istruzione.it

P.E.C. veic85000r@pec.istruzione.it

All' Assistente Amministrativo

.....
S E D E

Oggetto: **Nomina Incaricato al trattamento dei dati personali ai sensi dell'art. 30 D. Lgs. 196/2003 e dell'art. 4 Reg. UE n. 679/2016**

IL DIRIGENTE

- Visto il decreto legislativo n. 196/2003 (Codice in materia di protezione dei dati personali)
- Visto il Regolamento UE n. 679/2016 (G.D.P.R. General Data Protection Regulation)
- Preso atto che l'art. 4 comma 1 lett. h) del d.lgs. n. 196/2003 definisce "incaricati" le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- Preso atto che l'art. 4 n. 10) prevede la figura della "persona autorizzata al trattamento" dei dati personali;
- Premesso che il Garante ha statuito che "Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene opportuno che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento" [nota: <http://www.garanteprivacy.it/titolare-responsabile-incaricato-del-trattamento>]
- Preso atto che l'art. 30 del d. lgs. 196/2003 dispone che:

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito";

- Preso atto che l'art. 29 del Reg. UE 679/2016 dispone che:

"Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri";

- Preso atto che l'art. 32 comma 4 del Reg. UE 679/2016 dispone che:

"Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri";

DESIGNA

il sig./sig.ra. quale

INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

in relazione alle operazioni di elaborazione di dati personali, su supporto cartaceo e/o elettronico, ai quali il dipendente ha accesso nell'espletamento delle funzioni e dei compiti assegnati nell'ambito del rapporto di lavoro con questa istituzione scolastica e disciplinati dalla normativa in vigore e dai contratti di settore. In particolare, **in qualità di addetto alla Segreteria amministrativa e didattica della scuola** il dipendente è incaricato delle operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, comunicazione (nei soli casi autorizzati dal titolare o dal responsabile del trattamento), selezione, estrazione di dati, connesse alle seguenti funzioni e attività esercitate:

Alunni e genitori

- gestione archivi elettronici alunni e genitori;
- gestione archivi cartacei con fascicoli personali alunni;
- consultazione documenti e registri di attestazione dei voti e di documentazione della vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia quali ad esempio richieste, istanze e corrispondenza con le famiglie;
- gestione contributi e/o tasse scolastiche versati da alunni e genitori;
- adempimenti connessi alla corretta gestione del Registro infortuni;
- adempimenti connessi alle gite scolastiche;
- adempimenti vari connessi alla carriera scolastica degli alunni;

Personale ATA e Docenti

- gestione archivi elettronici Personale ATA e Docenti;
- gestione archivi cartacei Personale ATA e Docenti;
- tenuta documenti e registri relativi alla vita lavorativa dei dipendenti (quali ad es. assenze, convocazioni, comunicazioni, documentazione sullo stato del personale, atti di nomina dei supplenti, decreti del Dirigente);

Contabilità e finanza

- gestione archivi elettronici della contabilità;
- gestione stipendi e pagamenti, nonché adempimenti di carattere previdenziale;
- gestione documentazione ore di servizio (quali ad esempio, registrazione delle ore eccedenti);
- gestione rapporti con i fornitori;
- gestione Programma annuale e fondo di istituto
- corretta tenuta dei registri contabili previsti dal Decreto interministeriale n. 44/2001 e correlata normativa vigente.

Protocollo e archivio corrispondenza ordinaria

- attività di protocollo e archiviazione della corrispondenza ordinaria;

Attività organi collegiali

- eventuale operazione di consultazione e estrazione dati dai verbali degli organi collegiali.

Si rende noto, a tal fine, che le operazioni sopra descritte vanno rigorosamente effettuate tenendo presenti le istruzioni operative che seguono:

1. il trattamento dei dati personali cui il dipendente è autorizzato ad accedere deve avvenire secondo le modalità definite dalla normativa in vigore, in modo lecito e secondo correttezza

e con l'osservanza - in particolare - delle prescrizioni di cui al Regolamento UE 2016/679 e al Dlgs 196/2003;

2. il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola;
3. i dati personali, oggetto dei trattamenti, devono essere esatti ed aggiornati, inoltre devono essere pertinenti, completi e non eccedenti le finalità per le quali vengono raccolti e trattati;
4. è vietata qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia strettamente funzionale allo svolgimento dei compiti affidati. Si raccomanda particolare attenzione alla tutela del diritto alla riservatezza degli interessati (persone fisiche a cui afferiscono i dati personali);
5. si ricorda che l'obbligo di mantenere la dovuta riservatezza in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, deve permanere in ogni caso, anche quando sia venuto meno l'incarico stesso;
6. i trattamenti andranno effettuati rispettando le misure di sicurezza predisposte nell'istituzione scolastica; in ogni operazione di trattamento andrà garantita la massima riservatezza e custodia degli atti e dei documenti contenenti dati personali che non andranno mai lasciati incustoditi o a disposizione di terzi non autorizzati ad accedervi, prendervi visione o ad effettuare qualsivoglia trattamento;
7. le eventuali credenziali di autenticazione (codice di accesso e parola chiave per accedere ai computer e ai servizi web) attribuite alle SS.LL sono personali e devono essere custodite con cura e diligenza; non possono essere messe a disposizione né rivelate a terzi; non possono essere lasciate incustodite, né in libera visione. In caso di smarrimento e/o furto, bisogna darne immediata notizia al responsabile (o, in caso di assenza del responsabile, al titolare) del trattamento dei dati;
8. nel caso in cui per l'esercizio delle attività sopra descritte sia inevitabile l'uso di supporti rimovibili (quali ad esempio chiavi USB, CD-ROM, ecc), su cui sono memorizzati dati personali, essi vanno custoditi con cura, ne messi a disposizione o lasciati al libero accesso di persone non autorizzate;
9. si ricorda inoltre che i supporti rimovibili contenenti dati sensibili e/o giudiziari se non utilizzati vanno distrutti o resi inutilizzabili;
10. si ricorda inoltre che l'accesso agli archivi contenenti dati sensibili o giudiziari è permesso solo alle persone autorizzate e soggetto a continuo controllo secondo le regole definite dallo scrivente;
11. durante i trattamenti i documenti contenenti dati personali vanno mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate;
12. al termine del trattamento occorre custodire i documenti contenenti dati personali all'interno di archivi/cassetti/ armadi muniti di serratura;
13. i documenti della scuola contenenti dati personali non possono uscire dalla sede scolastica, né copiati, se non dietro espressa autorizzazione del responsabile o dal titolare del trattamento;
14. in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'incaricato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non incaricati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento;
15. le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata; se effettuate per scritto dovranno essere consegnate in contenitori chiusi;
16. all'atto della consegna di documenti contenenti dati personali l'incaricato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta
17. 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.

La presente designazione ha validità permanente (per tutto il tempo il cui il dipendente rimarrà in servizio presso l'Istituto) e pertanto non sarà soggetta a rinnovo annuale.

Il Dirigente Scolastico
Prof.ssa Sandra ZENNARO

Per ricevuta:

LINEE GUIDA IN MATERIA DI SICUREZZA PER il DSGA E L' ASSISTENTE AMMINISTRATIVO INCARICATO DEL TRATTAMENTO

Attenersi scrupolosamente alle seguenti indicazioni per garantire la sicurezza dei dati personali e, in particolare, dei dati sensibili e giudiziari:

- Conservare sempre i dati del cui trattamento si è incaricati in apposito armadio assegnato, dotato di serratura;
- Accertarsi della corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente al Titolare eventuali anomalie;
- Non consentire l'accesso alle aree in cui sono conservati dati personali su supporto cartaceo a estranei e a soggetti non autorizzati;
- Conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti;
- Consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti;
- Non consentire l'accesso a estranei al fax e alla stampante che contengano documenti non ancora ritirati dal personale;
- Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;
- Provvedere personalmente alla distruzione quando è necessario eliminare documenti inutilizzati;
- Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte;
- Non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici del personale e degli studenti e non annotarne il contenuto sui fogli di lavoro;
- Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati;
- Segnalare tempestivamente al Titolare la presenza di documenti incustoditi, provvedendo temporaneamente alla loro custodia;
- Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal Titolare.

Riguardo ai trattamenti eseguiti con supporto informatico attenersi scrupolosamente alle seguenti indicazioni:

- Non lasciare floppy disk, memorie usb e altri supporti, cartelle o altri documenti a disposizione di estranei;
- Conservare i dati sensibili in armadi chiusi, ad accesso controllato o in files protetti da password;
- Non consentire l'accesso ai dati a soggetti non autorizzati;
- Riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi;
- Scegliere una password con le seguenti caratteristiche:
 - originale
 - composta da almeno otto caratteri di cui almeno un numero una lettera un numero e un carattere speciale;
 - che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili
- curare la conservazione della propria password ed evitare di comunicarla ad altri;
- cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
- modificare prontamente la password assegnata dal custode delle credenziali;

- adottare le stesse cautele di cui sopra per le password di qualsiasi altra piattaforma software ad uso personale e potenzialmente interessata al Trattamento di Dati Personali (mail, account per piattaforme terze, eccetera);
- spegnere correttamente il computer al termine di ogni sessione di lavoro;
- non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- comunicare tempestivamente al Titolare qualunque anomalia riscontrata nel funzionamento del computer;
- non riutilizzare i supporti informatici utilizzati per il trattamento di dati sensibili per altri trattamenti;
- non gestire informazioni su più archivi ove non sia strettamente necessario e comunque curarne l'aggiornamento in modo organico;
- nella comunicazione multimediale per fini istituzionali con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall'Istituto; è fatto divieto utilizzare social network quali Facebook o altri;
- utilizzare le seguenti regole per la posta elettronica:
 - non aprire documenti di cui non sia certa la provenienza
 - non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
 - inviare messaggi di posta solo se espressamente autorizzati
 - controllare accuratamente l'indirizzo del destinatario o l'account qualora sia necessario inviare/condividere documenti contenenti dati personali
- nell'esercizio delle proprie mansioni utilizzare esclusivamente le apparecchiature informatiche fornite dalla scuola, presenti negli uffici di segreteria, in quanto tali attrezzature sono regolarmente sottoposte a rigide misure di sicurezza e in linea con le misure minime di sicurezza ICT emanate dall'AGID.

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



ISTITUTO COMPRENSIVO CHIOGGIA 3

SCUOLA INFANZIA - SCUOLA PRIMARIA – SCUOLA SECONDARIA DI 1° GRADO

Cod. Min. VEIC85000R Cod. - Fiscale 91020300272

Presidenza e Segreteria Via P. Togliatti, 831 - c.a.p. 30015 CHIOGGIA – VE

Tel. 041/400096 - e-mail veic85000r@istruzione.it

P.E.C. veic85000r@pec.istruzione.it

Al Direttore Servizi
Amministrativi Generali
Massimo PADOAN
S E D E

Oggetto: **Nomina Incaricato al trattamento dei dati personali ai sensi dell'art. 30 D. Lgs. 196/2003 e dell'art. 4 Reg. UE n. 679/2016**

IL DIRIGENTE

- Visto il decreto legislativo n. 196/2003 (Codice in materia di protezione dei dati personali)
- Visto il Regolamento UE n. 679/2016 (G.D.P.R. General Data Protection Regulation)
- Preso atto che l'art. 4 comma 1 lett. h) del d.lgs. n. 196/2003 definisce "incaricati" le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- Preso atto che l'art. 4 n. 10) prevede la figura della "persona autorizzata al trattamento" dei dati personali;
- Premesso che il Garante ha statuito che "Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene opportuno che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento" [nota: <http://www.garanteprivacy.it/titolare-responsabile-incaricato-del-trattamento>]
- Preso atto che l'art. 30 del d. lgs. 196/2003 dispone che:

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.
2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito";

- Preso atto che l'art. 29 del Reg. UE 679/2016 dispone che:

"Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri";

- Preso atto che l'art. 32 comma 4 del Reg. UE 679/2016 dispone che:

"Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri";

DESIGNA

il sig. Massimo PADOAN quale

INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

in relazione alle operazioni di elaborazione di dati personali, su supporto cartaceo e/o elettronico, ai quali il dipendente ha accesso nell'espletamento delle funzioni e dei compiti assegnati nell'ambito del rapporto di lavoro con questa istituzione scolastica e disciplinati dalla normativa in vigore e dai contratti di settore. In particolare, **in qualità di addetto alla Segreteria amministrativa e didattica della scuola** il dipendente è incaricato delle operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, comunicazione (nei soli casi autorizzati dal titolare o dal responsabile del trattamento), selezione, estrazione di dati, connesse alle seguenti funzioni e attività esercitate:

Alunni e genitori

- gestione archivi elettronici alunni e genitori;
- gestione archivi cartacei con fascicoli personali alunni;
- consultazione documenti e registri di attestazione dei voti e di documentazione della vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia quali ad esempio richieste, istanze e corrispondenza con le famiglie;
- gestione contributi e/o tasse scolastiche versati da alunni e genitori;
- adempimenti connessi alla corretta gestione del Registro infortuni;
- adempimenti connessi alle gite scolastiche;
- adempimenti vari connessi alla carriera scolastica degli alunni;

Personale ATA e Docenti

- gestione archivi elettronici Personale ATA e Docenti;
- gestione archivi cartacei Personale ATA e Docenti;
- tenuta documenti e registri relativi alla vita lavorativa dei dipendenti (quali ad es. assenze, convocazioni, comunicazioni, documentazione sullo stato del personale, atti di nomina dei supplenti, decreti del Dirigente);

Contabilità e finanza

- gestione archivi elettronici della contabilità;
- gestione stipendi e pagamenti, nonché adempimenti di carattere previdenziale;
- gestione documentazione ore di servizio (quali ad esempio, registrazione delle ore eccedenti);
- gestione rapporti con i fornitori;
- gestione Programma annuale e fondo di istituto
- corretta tenuta dei registri contabili previsti dal Decreto interministeriale n. 44/2001 e correlata normativa vigente.

Protocollo e archivio corrispondenza ordinaria

- attività di protocollo e archiviazione della corrispondenza ordinaria;

Attività organi collegiali

- eventuale operazione di consultazione e estrazione dati dai verbali degli organi collegiali.

In particolare, nel rispetto della normativa indicata nelle premesse, alla S.V. vengono affidate le seguenti responsabilità e compiti:

- Vigilare sul rispetto dell'incarico attribuito e sulle istruzioni specifiche impartite a tutti gli incaricati del trattamento dei dati personali;
- Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate da tutti i soggetti della S.V. incaricati del trattamento;
- Individuare, incaricare e nominare per iscritto, qualora la S.V. lo ritenga necessario, un Incaricato della gestione e della manutenzione degli strumenti elettronici, un Incaricato della custodia delle copie delle credenziali e un Incaricato delle copie di sicurezza delle banche dati;
- Verificare periodicamente le modalità di accesso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia ed accessibilità;
- Custodire e conservare i supporti utilizzati per le copie dei dati;
- Informare prontamente il titolare di ogni questione rilevante ai fini della normativa sulla privacy;
- Organizzare il servizio di consegna delle informative agli interessati e verificare che la stessa venga effettuata in tutti i casi previsti e ne sia garantita la registrazione;
- Verificare che per ogni trattamento, per il quale sia necessario acquisire il consenso dell'interessato, lo stesso sia richiesto e registrato;
- Verificare che le misure di sicurezza adottate siano costantemente adeguate agli aggiornamenti legislativi e al progresso tecnico.

In funzione dell'incarico conferito, sarà inoltre cura della S.V. verificare:

- che il trattamento dei dati da parte del personale posto alle dirette dipendenze avvenga in modo lecito e secondo correttezza;
- che la raccolta e la registrazione avvengano: per scopi determinati e legittimi ed in modo compatibile con tali scopi e nell'ambito del trattamento necessario per il funzionamento dell'istituzione scolastica; in modo esatto e se necessario con gli opportuni aggiornamenti; in modo che essi risultino pertinenti, completi e non eccedenti rispetto alle finalità di raccolta; in modo che la loro conservazione sia funzionale al periodo di tempo necessario allo scopo per il quale sono stati raccolti e successivamente trattati.

Si rende noto, a tal fine, che le operazioni sopra descritte vanno rigorosamente effettuate tenendo presenti le istruzioni operative che seguono:

1. il trattamento dei dati personali cui il dipendente è autorizzato ad accedere deve avvenire secondo le modalità definite dalla normativa in vigore, in modo lecito e secondo correttezza e con l'osservanza - in particolare - delle prescrizioni di cui al Regolamento UE 2016/679 e al Dlgs 196/2003;
2. il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola;
3. i dati personali, oggetto dei trattamenti, devono essere esatti ed aggiornati, inoltre devono essere pertinenti, completi e non eccedenti le finalità per le quali vengono raccolti e trattati;
4. è vietata qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia strettamente funzionale allo svolgimento dei compiti affidati. Si raccomanda particolare attenzione alla tutela del diritto alla riservatezza degli interessati (persone fisiche a cui afferiscono i dati personali);
5. si ricorda che l'obbligo di mantenere la dovuta riservatezza in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, deve permanere in ogni caso, anche quando sia venuto meno l'incarico stesso;
6. i trattamenti andranno effettuati rispettando le misure di sicurezza predisposte nell'istituzione scolastica; in ogni operazione di trattamento andrà garantita la massima riservatezza e custodia degli atti e dei documenti contenenti dati personali che non andranno mai lasciati incustoditi o a disposizione di terzi non autorizzati ad accedervi, prendervi visione o ad effettuare qualsivoglia trattamento;

7. le eventuali credenziali di autenticazione (codice di accesso e parola chiave per accedere ai computer e ai servizi web) attribuite alle SS.LL sono personali e devono essere custodite con cura e diligenza; non possono essere messe a disposizione né rivelate a terzi; non possono essere lasciate incustodite, né in libera visione. In caso di smarrimento e/o furto, bisogna darne immediata notizia al responsabile (o, in caso di assenza del responsabile, al titolare) del trattamento dei dati;
8. nel caso in cui per l'esercizio delle attività sopra descritte sia inevitabile l'uso di supporti rimovibili (quali ad esempio chiavi USB, CD-ROM, ecc), su cui sono memorizzati dati personali, essi vanno custoditi con cura, ne messi a disposizione o lasciati al libero accesso di persone non autorizzate;
9. si ricorda inoltre che i supporti rimovibili contenenti dati sensibili e/o giudiziari se non utilizzati vanno distrutti o resi inutilizzabili;
10. si ricorda inoltre che l'accesso agli archivi contenenti dati sensibili o giudiziari è permesso solo alle persone autorizzate e soggetto a continuo controllo secondo le regole definite dallo scrivente;
11. durante i trattamenti i documenti contenenti dati personali vanno mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate;
12. al termine del trattamento occorre custodire i documenti contenenti dati personali all'interno di archivi/cassetti/ armadi muniti di serratura;
13. i documenti della scuola contenenti dati personali non possono uscire dalla sede scolastica, né copiati, se non dietro espressa autorizzazione del responsabile o dal titolare del trattamento;
14. in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'incaricato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non incaricati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento;
15. le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata; se effettuate per scritto dovranno essere consegnate in contenitori chiusi;
16. all'atto della consegna di documenti contenenti dati personali l'incaricato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta
17. 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.

La presente designazione ha validità permanente (per tutto il tempo in cui il dipendente rimarrà in servizio presso l'Istituto) e pertanto non sarà soggetta a rinnovo annuale.

Il Dirigente Scolastico
Prof.ssa Sandra ZENNARO

Per ricevuta:

LINEE GUIDA IN MATERIA DI SICUREZZA PER L' ASSISTENTE AMMINISTRATIVO INCARICATO DEL TRATTAMENTO

Attenersi scrupolosamente alle seguenti indicazioni per garantire la sicurezza dei dati personali e, in particolare, dei dati sensibili e giudiziari:

- Conservare sempre i dati del cui trattamento si è incaricati in apposito armadio assegnato, dotato di serratura;
- Accertarsi della corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente al Titolare eventuali anomalie;
- Non consentire l'accesso alle aree in cui sono conservati dati personali su supporto cartaceo a estranei e a soggetti non autorizzati;
- Conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti;
- Consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti;
- Non consentire l'accesso a estranei al fax e alla stampante che contengano documenti non ancora ritirati dal personale;
- Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;
- Provvedere personalmente alla distruzione quando è necessario eliminare documenti inutilizzati;
- Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte;
- Non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici del personale e degli studenti e non annotarne il contenuto sui fogli di lavoro;
- Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati;
- Segnalare tempestivamente al Titolare la presenza di documenti incustoditi, provvedendo temporaneamente alla loro custodia;
- Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal Titolare.

Riguardo ai trattamenti eseguiti con supporto informatico attenersi scrupolosamente alle seguenti indicazioni:

- Non lasciare floppy disk, memorie usb e altri supporti, cartelle o altri documenti a disposizione di estranei;
- Conservare i dati sensibili in armadi chiusi, ad accesso controllato o in files protetti da password;
- Non consentire l'accesso ai dati a soggetti non autorizzati;
- Riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi;
- Scegliere una password con le seguenti caratteristiche:
- originale
- composta da almeno otto caratteri di cui almeno un numero una lettera un numero e un carattere speciale;
- che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili
- curare la conservazione della propria password ed evitare di comunicarla ad altri;
- cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;

- modificare prontamente la password assegnata dal custode delle credenziali;
- adottare le stesse cautele di cui sopra per le password di qualsiasi altra piattaforma software ad uso personale e potenzialmente interessata al Trattamento di Dati Personali (mail, account per piattaforme terze, eccetera);
- spegnere correttamente il computer al termine di ogni sessione di lavoro;
- non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- comunicare tempestivamente al Titolare qualunque anomalia riscontrata nel funzionamento del computer;
- non riutilizzare i supporti informatici utilizzati per il trattamento di dati sensibili per altri trattamenti;
- non gestire informazioni su più archivi ove non sia strettamente necessario e comunque curarne l'aggiornamento in modo organico;
- nella comunicazione multimediale per fini istituzionali con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall'Istituto; è fatto divieto utilizzare social network quali Facebook o altri;
- utilizzare le seguenti regole per la posta elettronica:
 - non aprire documenti di cui non sia certa la provenienza
 - non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
 - inviare messaggi di posta solo se espressamente autorizzati
 - controllare accuratamente l'indirizzo del destinatario o l'account qualora sia necessario inviare/condividere documenti contenenti dati personali
- nell'esercizio delle proprie mansioni utilizzare esclusivamente le apparecchiature informatiche fornite dalla scuola, presenti negli uffici di segreteria, in quanto tali attrezzature sono regolarmente sottoposte a rigide misure di sicurezza e in linea con le misure minime di sicurezza ICT emanate dall'AGID.

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

LINEE GUIDA IN MATERIA DI SICUREZZA PER IL DSGA INCARICATO DEL TRATTAMENTO

Attenersi scrupolosamente alle seguenti indicazioni per garantire la sicurezza dei dati personali e, in particolare, dei dati sensibili e giudiziari:

- Conservare sempre i dati del cui trattamento si è incaricati in apposito armadio assegnato, dotato di serratura;
- Accertarsi della corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente al Titolare eventuali anomalie;
- Non consentire l'accesso alle aree in cui sono conservati dati personali su supporto cartaceo a estranei e a soggetti non autorizzati;
- Conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti;
- Consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti;
- Non consentire l'accesso a estranei al fax e alla stampante che contengano documenti non ancora ritirati dal personale;
- Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;
- Provvedere personalmente alla distruzione quando è necessario eliminare documenti inutilizzati;
- Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte;
- Non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici del personale e degli studenti e non annotarne il contenuto sui fogli di lavoro;
- Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati;
- Segnalare tempestivamente al Titolare la presenza di documenti incustoditi, provvedendo temporaneamente alla loro custodia;
- Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal Titolare.

Riguardo ai trattamenti eseguiti con supporto informatico attenersi scrupolosamente alle seguenti indicazioni:

- Non lasciare floppy disk, memorie usb e altri supporti, cartelle o altri documenti a disposizione di estranei;
- Conservare i dati sensibili in armadi chiusi, ad accesso controllato o in files protetti da password;
- Non consentire l'accesso ai dati a soggetti non autorizzati;
- Riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi;
- Scegliere una password con le seguenti caratteristiche:
 - originale
 - composta da almeno otto caratteri di cui almeno un numero una lettera un numero e un carattere speciale;
 - che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili
 - curare la conservazione della propria password ed evitare di comunicarla ad altri;
 - cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
 - modificare prontamente la password assegnata dal custode delle credenziali;
 - adottare le stesse cautele di cui sopra per le password di qualsiasi altra piattaforma software ad uso personale e potenzialmente interessata al Trattamento di Dati Personali (mail, account per piattaforme terze, eccetera);
- spegnere correttamente il computer al termine di ogni sessione di lavoro;

- non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- comunicare tempestivamente al Titolare qualunque anomalia riscontrata nel funzionamento del computer;
- non riutilizzare i supporti informatici utilizzati per il trattamento di dati sensibili per altri trattamenti;
- non gestire informazioni su più archivi ove non sia strettamente necessario e comunque curarne l'aggiornamento in modo organico;
- nella comunicazione multimediale per fini istituzionali con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall'Istituto; è fatto divieto utilizzare social network quali Facebook o altri;
- utilizzare le seguenti regole per la posta elettronica:
 - non aprire documenti di cui non sia certa la provenienza
 - non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
 - inviare messaggi di posta solo se espressamente autorizzati
 - controllare accuratamente l'indirizzo del destinatario o l'account qualora sia necessario inviare/condividere documenti contenenti dati personali
- nell'esercizio delle proprie mansioni utilizzare esclusivamente le apparecchiature informatiche fornite dalla scuola, presenti negli uffici di segreteria, in quanto tali attrezzature sono regolarmente sottoposte a rigide misure di sicurezza e in linea con le misure minime di sicurezza ICT emanate dall'AGID.

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