ISTITUTO COMPRENSIVO A. GRANDI-
C.F. 93173040754 C.M. LEIC8AV008
PTCS2025 - I.C. Grandi - Castromediano
Prot. 0010402/U del 04/09/2026 08:26

ISTITUTO COMPRENSIVO STATALE
AD INDIRIZZO MUSICALE
A. GRANDI - S. CASTROMEDIANO

Via F.sco Patitari, 2 - 73100 - Lecce • Tel 0832/346889 - Fax: 0832/231441 • CF: 93173040754 • COD.MEC.LEIC8AV008
PEO: leic9av008@istruzione.it • PEC: leic8av008@pec.istruzione.it

DECRETO DIRIGENZIALE DEL DIRIGENTE SCOLASTICO

Numero 2 - del 03/09/26

ATTO DI AUTORIZZAZIONE

– Misure finalizzate alla corretta attuazione alle disposizioni del Regolamento (UE) 679/2016 e del D.Lgs. 196/2003 così come modificato e novellato dal D.Lgs. 101/2018 –

OGGETTO: Nomina delle Persone Autorizzate al trattamento dei dati personali, ai sensi degli artt. 4 e 29 del Regolamento Europeo 679/2016 e integrazione delle istruzioni al personale dipendente.

IL DIRIGENTE SCOLASTICO

Visto il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (di seguito solo GDPR);

Visto il D.Lgs. 30 Giugno 2003, n.196 "Codice in materia di protezione dei dati personali";

Visto il D.Lgs. del 10 Agosto 2018 n.101 "Adeguamento al Regolamento UE 2016/679";

Visto il D.P.R. 13 giugno 2023, n. 81, Regolamento concernente modifiche al decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165».;

Visto il D.Lgs. 7 marzo 2005, n. 82 "Codice dell'Amministrazione Digitale" e ss.mm.ii.;

Rilevato che, ai fini dell'osservanza delle disposizioni contenute nel GDPR, vanno innanzitutto individuati gli attori, i ruoli e le responsabilità del sistema organizzativo preordinato a garantire la protezione dei dati personali;

Richiamati gli articoli 4 e 29 del Regolamento Europeo 679/2016, che in particolare dispongono:

Art. 4 (definizioni)

"[…] ... «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;

Art. 29 (Trattamento sotto l'autorità del Titolare del trattamento […])

"[…] ... 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 … […]

Constatato che:

Via F.sco Patitari, 2 - 73100 - Lecce • Tel 0832/346889 - Fax: 0832/231441 • CF: 93173040754 • COD.MEC.LEIC8AV008
PEO: leic9av008@istruzione.it • PEC: leic8av008@pec.istruzione.it

- è necessario attuare la migliore qualità conseguibile nel trattamento dei dati personali e ciò è possibile attuando in piena autonomia la gestione dei compiti all'interno della scuola;

- Risulta necessario configurare l'articolazione scolastica, secondo criteri di efficienza e efficacia, delegando compiti operativi a personale che possieda abilità e formazione opportune per svolgere le mansioni a esso delegate;

DISPONE

1) Di individuare il personale con il ruolo di "**COLLABORATORE SCOLASTICO**" quali Persone autorizzate al trattamento (ex artt. 4 e 29 del Regolamento Europeo 679/2016)" per i trattamenti necessari per l'espletamento delle mansioni ricoperte all'interno della Scuola.

2) Di autorizzare questa categoria di persone autorizzate a trattare solo i dati personali di natura comune (anagrafiche e dati di contatto) ed eventualmente le categorie particolari di dati personali di cui all'art. 9 del Regolamento Ue 2016/679 con cui entrino in contatto nell'ambito dell'espletamento dell'attività di loro competenza o contenuti nelle banche dati, in archivi cartacei e informatici dell'Istituto; in particolare, in qualità di Collaboratori scolastici dell'istituto alle SS.LL può essere affidata temporaneamente la custodia, lo spostamento, l'archiviazione o la riproduzione di documenti contenenti dati personali, nonché la ricezione di documentazione da parte delle famiglie degli alunni.

3) Per lo svolgimento delle suddette operazioni potrà avrà accesso a postazioni informatiche e caselle di posta elettronica (personali e/o condivise), nonché ad applicazioni software per la gestione delle mansioni lavorative.

4) Di dare atto che ogni dipendente che cessa di far parte o perde il ruolo di "Collaboratore scolastico" cessa automaticamente dalla funzione di persona autorizzata al trattamento.

5) Ogni nuovo dipendente che entra a far parte o assume il ruolo di "Collaboratore scolastico" assume automaticamente la funzione di persona autorizzata al trattamento e che, pertanto, l'elenco delle persone autorizzate appartenenti a questa categoria corrisponde all'elenco dei dipendenti validamente in servizio che ne fanno parte.

6) Di autorizzare il personale con il ruolo di "Collaboratore scolastico" a trattare i dati suddetti nel rispetto di tutte le misure di sicurezza previste dalla legge ed in particolare dal Regolamento UE 2016/679.

7) Di mettere a disposizione tutto il materiale informativo e legislativo necessario per approfondire la conoscenza della materia, nonché di organizzare appositi corsi di formazione in materia di privacy.

8) Di consegnare, all'atto dell'assunzione in servizio, a ogni nuovo componente (anche temporaneo) con il ruolo di "Collaboratore scolastico" copia della presente determina.

9) Di puntualizzare che i compiti e le funzioni a tal fine assegnate sono analiticamente elencate in calce al presente provvedimento, con facoltà di successiva integrazione e/o modificazione, dando atto che l'attribuzione di compiti e funzioni inerenti al trattamento dei dati personali non implica l'attribuzione di compiti e funzioni ulteriori rispetto a quelli propri della qualifica rivestita ma

conferisce soltanto il potere/dovere di svolgere i compiti le funzioni attribuite.

10) Di dare atto, altresì, che:

- tale ruolo ha validità per l'intera durata del rapporto / incarico di dipendenza;
- tale ruolo viene a cessare al modificarsi del rapporto / incarico di dipendenza;
- tale ruolo viene a cessare in caso di revoca espressa;
- tale ruolo non consente l'attribuzione ad altri soggetti di poteri e compiti qui previsti;
- al cessare di tale ruolo, rimane inibito e comunque non autorizzato ogni ulteriore esercizio dei compiti e delle funzioni trattamento dei dati personali oggetto del presente provvedimento, salvo che ciò sia imposto o consentito da una norma di Legge o da un provvedimento dell'autorità ovvero sia necessario ad esercitare o difendere un diritto.

NOTIFICA E COMUNICAZIONE DEL PRESENTE ATTO

La presente dovrà essere comunicata ai destinatari sopra "Autorizzati" a mezzo PEO/PEC/Registro Elettronico o altre modalità individuate dalla Scuola

Lecce, 03/09/26

IL DIRIGENTE SCOLASTICO

dott.ssa Maria Rosaria Manca

Documento informatico sottoscritto con firma digitale (*ex art. 24 D.Lgs. n.82 del 07/03/2005*)

Firmato digitalmente da Maria Rosaria Manca
C: IT

Via F.sco Patitari, 2 - 73100 - Lecce • Tel 0832/346889 - Fax: 0832/231441 • CF: 93173040754 • COD.MEC.LEIC8AV008
PEO: leic9av008@istruzione.it • PEC: leic8av008@pec.istruzione.it

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

ISTRUZIONI GENERALI

Nello svolgere le proprie funzioni, che comportino un trattamento di dati personali, il personale scolastico deve attenersi alle seguenti istruzioni:

1. le persone autorizzate al trattamento devono operare sotto la diretta autorità del Titolare del trattamento e devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni ricevute;
2. qualunque trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali dell'Istituto;
3. è vietata qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia strettamente funzionale allo svolgimento dei compiti affidati e comunque autorizzata dal titolare del trattamento, o da una norma di legge o di regolamento;
4. i collaboratori scolastici autorizzati al trattamento hanno l'obbligo di mantenere il riserbo sulle informazioni di cui siano venuti a conoscenza nell'esercizio della loro funzione; tale obbligo permane anche dopo la cessazione dell'incarico, senza limiti temporali;
5. devono essere rispettate ed applicate tutte le misure di sicurezza previste dalla legge ed in particolare dal Regolamento UE 2016/679;
6. i dati personali devono essere trattati in modo lecito e corretto secondo le prescrizioni di cui al Reg. UE 679/16, nel rispetto dei principi generali di liceità, correttezza, trasparenza, esattezza, minimizzazione e di quanto riportato nel Registro delle Attività di Trattamento adottato dall'Istituto scolastico;
7. 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;
8. le persone autorizzate al trattamento sono tenute a partecipare agli interventi formativi organizzati dalla Istituto scolastico sui profili della disciplina sulla protezione dei dati personali in rapporto alle attività connesse alle loro mansioni;
9. le persone autorizzate al trattamento devono attenersi alle seguenti modalità operative: richiedere e utilizzare soltanto i dati necessari alla normale attività lavorativa; custodire i dati oggetto di trattamento in luoghi sicuri e non accessibili ai soggetti non autorizzati; non lasciare incustoditi i documenti e gli altri supporti, anche informatici, contenenti dati personali senza aver provveduto alla loro messa in sicurezza; provvedere alla tempestiva riconsegna della documentazione consultata per causa di lavoro a chi è incaricato della sua conservazione permanente; accertarsi dell'identità di

terzi e della loro autorizzazione al ritiro della documentazione in uscita; non consentire che estranei possano accedere ai documenti o leggere documenti contenenti dati personali;

10. le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata; se effettuate per scritto dovranno essere consegnate busta chiusa;

11. segnalare tempestivamente al Responsabile del trattamento la presenza di documenti incustoditi e provvedere temporaneamente alla loro custodia;

12. accertarsi che al termine delle lezioni non rimangano incustoditi i seguenti documenti, provvedendo temporaneamente alla loro custodia e segnalando la situazione tempestivamente al Responsabile: registro personale docenti; registro di classe; certificati medici esibiti dagli alunni a giustificazione delle assenze, altri documenti contenenti dati personali o le categorie particolari di dati personali di cui all'art .9 del Regolamento Ue 2016/679 degli alunni o dei docenti;

13. accertarsi che al termine delle lezioni tutti i computer dell'aula di informatica siano spenti e che non siano lasciati incustoditi materiali, in caso contrario provvedere temporaneamente alla loro custodia e segnalare la situazione tempestivamente al DSGA;

14. verificare la corretta funzionalità dei meccanismi di chiusura di armadi che custodiscono dati personali, segnalando tempestivamente al Responsabile eventuali anomalie;

15. all'atto della consegna di documenti contenenti dati personali la persona autorizzata al trattamento dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta;

16. procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei locali siano state attivate e che le chiavi delle stanze siano depositate negli appositi contenitori;

17. i documenti della scuola contenenti dati personali non possono essere portati all'esterno della sede scolastica, né copiati, se non previa espressa autorizzazione del responsabile o dal titolare del trattamento;

18. il trattamento di eventuali categorie particolari di dati personali di cui all'art. 9 del Regolamento Ue 2016/679 è consentito nei limiti e secondo le modalità di cui all'art. 9 del Regolamento stesso; i supporti e la documentazione contenenti tale tipologia di dati devono essere utilizzati con particolare accortezza e nel pieno rispetto delle misure di sicurezza apprestate dal Titolare;

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

Qualunque violazione delle istruzioni operative indicate nel presente documento dà luogo a precise responsabilità, anche disciplinari, ai sensi delle norme contenute nel Regolamento UE 679/2016 e dell'art. 4 dello Statuto dei Lavoratori.

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

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

A) CREDENZIALI DI AUTENTICAZIONE INFORMATICA
(Password, username e accesso ai sistemi informatici)

1. le credenziali di autenticazione informatica sono individuali 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;

2. è vietato comunicare a terzi gli esiti delle proprie interrogazioni delle banche dati;
3. i codici identificativi, le *password* e le *smart card* saranno disattivate nel caso in cui i dipendenti cessino il loro rapporto di lavoro, oltre che nei casi espressamente e tassativamente previsti dalla normativa. In tali casi il dipendente è tenuto a restituirle agli uffici a ciò preposti.
4. la *password* che la persona fisica designata e autorizzata al trattamento imposta, con il supposto e l'assistenza, in caso di difficoltà, dell'Amministratore di Sistema (se esistente):
5. deve essere sufficientemente lunga e complessa e deve contemplare l'utilizzo di caratteri maiuscoli e speciali e numeri (almeno 10 caratteri);
   - non deve essere riconducibile alla persona;
   - deve essere cambiata almeno ogni 3/6 mesi;
   - non deve essere rivelata o fatta digitare al personale di assistenza tecnica;
   - non deve essere rivelata o comunicata al telefono, via fax od altra modalità elettronica;
   - non memorizzare *password* su dispositivi dell'Istituto o apparecchiature personali;
6. se si utilizza un PC condiviso, avere cura di accedere con il proprio *account* e disconnetterlo al termine dell'utilizzo;
7. eseguire sempre il corretto *logout* dagli account personali al termine della sessione di lezione, per evitare accessi non autorizzati e garantire la riservatezza dei dati trattati (es. registro elettronico e/o *account* personale piattaforme multimediali);
8. trattare i dati personali mediante l'utilizzo di apparecchiature in possesso dell'Istituzione scolastica;
9. non memorizzare dati personali su dispositivi dell'Istituto o apparecchiature personali;

Via F.sco Patitari, 2 - 73100 - Lecce • Tel 0832/346889 - Fax: 0832/231441 • CF: 93173040754 • COD.MEC.LEIC8AV008
PEO: leic9av008@istruzione.it • PEC: leic8av008@pec.istruzione.it

10. in caso di perplessità in merito alla scelta delle soluzioni comportamentali più corrette da adottare, le persone autorizzate devono consultarsi con il Titolare o con il Responsabile onde evitare di incorrere in violazioni di legge;

11. informare tempestivamente il Titolare o il responsabile del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata;

B) POSTA ELETTRONICA

1. la casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell'ambito dell'attività lavorativa;

2. l'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione della Scuola. L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti al servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale;

3. si invitano i dipendenti a non utilizzare gli indirizzi di posta elettronica istituzionali assegnati per le comunicazioni personali;

4. le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta nel rispetto della normativa vigente;

5. non è consentito inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o che possano essere in qualunque modo fonte di responsabilità della Scuola;

6. il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dalla Scuola. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile;

7. la posta elettronica diretta all'esterno della rete della Scuola può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti contenenti dati personali di cui agli articoli 9 e 10 del GDPR;

8. non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale della Scuola per la partecipazione a dibattiti, Forum o mail-list, salvo diversa ed esplicita autorizzazione;

9. qualora si verifichino anomalie nell'invio e ricezione dei messaggi di posta elettronica sarà cura del dipendente informare prontamente l'Amministratore di sistema o il Dirigente scolastico;

10. 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;

11. nei casi di inoltro di e-mail a più destinatari esterni al Titolare che non hanno l'esigenza di conoscere gli altri destinatari, occorre utilizzare la funzionalità di invio per copia conoscenza nascosta (*ccn*).

C) ISTRUZIONI PER IL TRATTAMENTO DI DATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

1. Le pratiche e i fascicoli contenenti dati personali (di seguito: "le pratiche") devono essere di norma riposte in archivi chiusi. Si considera archivio chiuso anche il locale chiuso a chiave;

2. le pratiche e i fascicoli devono essere prelevati, a cura degli utilizzatori, solo nella misura e per il tempo strettamente necessari per lo svolgimento dei relativi compiti, al termine dei quali – ed in ogni caso al termine della giornata lavorativa – devono essere riposte negli archivi. Ciascun utilizzatore deve aver cura di verificare che le pratiche affidategli non restino incustodite, specie in contesti accessibili a soggetti non incaricati del trattamento (aree di passaggio, sale d'attesa, sale riunioni, ecc.);

3. anche durante la giornata lavorativa, in caso di allontanamento dalla postazione di lavoro per un periodo di tempo significativo, le pratiche devono essere riposte negli archivi, salvo adeguata garanzia di controllo da parte di altri utilizzatori autorizzati ai medesimi trattamenti. In ogni caso le pratiche non devono essere mai lasciate incustodite;

4. lo smarrimento o il furto di informazioni devono essere comunicati immediatamente ai referenti della procedura sui Data Breach;

5. è buona regola evitare la proliferazione eccessiva di stampe e fotocopie di documenti contenenti dati personali. Effettuare esclusivamente copie fotostatiche di documenti per i quali si è stati autorizzati. Le stampe e le fotocopie inutili devono essere distrutte nell'apposito distruggi-documenti, se disponibile, oppure devono essere strappate in pezzi piccoli;

6. oltre a quanto previsto per i dati personali in genere, le pratiche e i fascicoli contenenti categorie particolari di dati e dati relativi a condanne penali o reati devono essere conservati in archivi ad accesso controllato, devono essere controllate e custodite fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione (ivi compresi altri utilizzatori che non siano autorizzati ad accedere alle informazioni sensibili), e devono essere restituite al termine delle operazioni affidate;

7. quando circolano all'interno dell'Istituto scolastico devono essere inserite in busta chiusa; stesso discorso qualora vi fosse la necessità di comunicare tali dati e documenti ad altri Enti (es. Comuni o ASL) autorizzati in forza di norma di legge o regolamento a riceverli;

8. compete agli utilizzatori il controllo della chiusura a chiave degli armadi contenenti tale tipologia di dati e la chiusura dei propri uffici in caso di temporaneo allontanamento ed alla fine dell'orario lavorativo. I documenti contenenti dati ultra-sensibili (es. stato di salute relativo ad alunni con BES o DSA) devono essere custoditi in cassaforte o in archivio separato.

Via F.sco Patitari, 2 - 73100 - Lecce • Tel 0832/346889 - Fax: 0832/231441 • CF: 93173040754 • COD.MEC.LEIC8AV008
PEO: leic9av008@istruzione.it • PEC: leic8av008@pec.istruzione.it

Gestione chiavi

1. I soggetti chiamati a gestire le chiavi "fisiche" degli archivi devono:
2. all'atto della consegna delle chiavi, verificarne subito il corretto funzionamento;
3. verificare che le chiavi non restino inserite negli armadi/archivi;
4. conservare le chiavi in un luogo e con modalità che ne garantiscano una sicurezza adeguata anche al tipo di archivio;
5. non metterle a disposizione né mostrarle ad estranei;
6. in caso di smarrimento o sottrazione, farne immediata segnalazione ai referenti delle procedura sui Data Breach e richiedere la sollecita sostituzione della serratura, spostando se del caso, per il tempo necessario, i documenti dall'archivio non protetto.
7. Compete a tali soggetti il controllo della chiusura a chiave degli armadi contenenti dati sensibili e la chiusura dei propri uffici in caso di temporaneo allontanamento ed alla fine dell'orario lavorativo

Scarti di archivio

1. Gli scarti di archivio, ossia il periodico smaltimento di materiale cartaceo contenente dati personali, deve essere effettuato evitando che le informazioni personali, specie se sensibili, possano essere trattate da soggetti non incaricati/autorizzati.
2. In particolare i documenti contenenti categorie particolari si dati devono essere smaltiti mediante utilizzo degli appositi strumenti per la distruzione, ove disponibili, altrimenti vanno ridotti in piccoli pezzi.

Consegna di certificazioni medico-sanitarie a mezzo di altri soggetti

1. La consegna di certificazioni mediche, o comunque di altre informazioni personali delicate relative ai dipendenti, alunni o terzi può essere effettuata anche tramite altri dipendenti o comunque altre persone a condizione che:
   - la documentazione sia di regola consegnata in busta chiusa;
   - prima della consegna, la documentazione non sia lasciata incustodita. Di regola, ove non sia presente il destinatario, la documentazione va consegnata a un responsabile o superiore gerarchico;
   - la consegna avvenga nel minor tempo possibile.

Centralino, telefonate e colloqui

1. Il personale addetto al centralino deve considerare che il colloquio telefonico non è, di norma, metodo adeguato all'identificazione sicura dell'interlocutore.

2. Deve essere pertanto rispettata la seguente regola generale: non è consentito fornire informazioni personali telefonicamente, in quanto non è di norma possibile identificare con certezza la persona con la quale è in corso il colloquio.
3. La regola generale può trovare eccezioni tutte le volte in cui si possa ragionevolmente ritenere di avere sufficienti elementi per l'identificazione certa dell'interlocutore (ad esempio, in quanto esiste con l'interlocutore una consuetudine di rapporto, tale da garantire di fatto il riconoscimento; oppure in forza di una verifica su alcuni dati personali –data di nascita, codice fiscale, ecc.; e così via).
4. Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, anche utilizzando cellulari, per evitare che dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.

D) ISTRUZIONI DA SEGUIRE IN CASO DI DATA BREACH

Nel caso in cui vi sia il fondato sospetto che si sia verificata una violazione di dati, come ad esempio:

- Perdita di documenti o fascicoli
- Distruzione archivi
- Furto o smarrimento di strumenti elettronici contenenti dati personali
- Sospetto di accesso non autorizzato nei locali deputati all'archiviazione
- Sospetto di accesso non autorizzato nella sala Server
- Sospetto di accesso non autorizzato nel proprio PC
- Comportamento anomalo del proprio PC o dispositivo informatico
- Etc.…

Occorre informare tempestivamente i referenti della procedura sui Data Breach, comunicandogli il maggior numero di dettagli circa la violazione subita:

- Data in cui è avvenuto l'evento o in cui si è venuti a conoscenza.
- Modalità di esposizione al rischio, ad es.: Lettura dei dati personali, Copia dei dati personali, Alterazioni dei dati personali, Cancellazione dei dati personali, Furto dei dati personali.
- Dati personali oggetto della violazione (dati dei dipendenti, degli alunni etc.).