



Ministero dell'Istruzione e del Merito
Ufficio Scolastico Regionale per la Campania
Istituto Comprensivo Statale "ITALO CALVINO"

Via Bologna, 57 – 80010 VILLARICCA (NA) -
www.calvinovillaricca.edu.it cod. mecc. NAIC885001 – cod. fisc.
95020120630

e-mail: naic885001@istruzione.it; pec.naic885001@pec.istruzione.it tel. 081/818.16.85

Prot. n., vedi segnatura

Villaricca, vedi segnatura

Circ.n.54/A.S. 2026- 2027

- Ai Docenti.
E p.c.
- Al DSGA;
- Al personale Amministrativo
 - Area della Didattica;
- Alla I e II Collaboratrice del Dirigente;
- Alla F. S. Inclusione
- Alle Referenti Sostegno
LORO Sedi;
- Agli Atti

OGGETTO: Introduzione del PEI digitale sulla piattaforma SIDI – a.s. 2026/2027

Si informa che, a partire dall'anno scolastico 2025/2026, l'Istituto ha adottato in via ufficiale il Piano Educativo Individualizzato (PEI) in formato digitale, attraverso la piattaforma ministeriale SIDI (Sistema Informativo Dell'Istruzione), come previsto dalle disposizioni del Ministero dell'Istruzione e del Merito in materia di digitalizzazione dei documenti scolastici.

Tale innovazione mira a:

- semplificare la gestione e la condivisione del documento tra scuola, famiglia e specialisti;
- garantire maggiore trasparenza, tracciabilità e tutela dei dati personali;
- favorire una compilazione più chiara e coordinata tra i diversi soggetti coinvolti nel progetto educativo personalizzato dell'alunno.

In questa fase di avvio dei lavori appare opportuno richiamare all'attenzione del Personale interessato i principi cardine dell'azione amministrativa a tutela del rigoroso rispetto degli obblighi relativi al trattamento dati e delle procedure.

1. Separazione tra autorizzati interni e soggetti esterni

Non useremo più la formula generica secondo cui **"tutti i componenti GLO sono autorizzati dalla scuola"**.

La scuola autorizza il proprio personale secondo l'art. 29 GDPR; per i soggetti esterni si verifica invece la loro specifica posizione giuridica e il titolo che legittima la partecipazione.

2. Registro GLO come evidenza di accountability

Non basta dire che "la scuola gestisce gli accessi". Deve poter dimostrare **chi era componente, perché, da quando, con quale ruolo e con quale livello di accesso.**

3. Accessi SIDI collegati alla composizione effettiva del GLO

Questo è particolarmente importante perché il documento ministeriale stesso evidenzia che i componenti vengono registrati e abilitati e che il livello di autorizzazione determina se possono visualizzare, modificare o sottoscrivere. cds_171_PEI_DIGITALE_SIDI

4. Convocazione GLO = informazione sanitaria

Questo deve diventare un principio espresso nella procedura e non una semplice raccomandazione. È ormai sostenuto da più provvedimenti del Garante.

5. Divieto di pubblicazione molto più preciso

Non dobbiamo limitarci a scrivere “non pubblicare il PEI”.

La procedura deve vietare anche la pubblicazione o comunicazione generalizzata di **convocazioni GLO, riferimenti al PEI, elenchi, circolari nominative e informazioni contestuali idonee a rivelare la disabilità**. Il provvedimento del Garante del 29 gennaio 2026 rende questo punto particolarmente importante.

6. Data Breach non significa automaticamente notifica al Garante

La procedura corretta è:

incidente → segnalazione → contenimento → analisi → valutazione del rischio → decisione sulla notifica ex art. 33 → eventuale comunicazione ex art. 34 → registrazione dell'evento.

Non ogni incidente deve essere notificato al Garante, ma **ogni violazione deve essere valutata e documentata**.

7. Collegamento tra i sei documenti

A questo punto il sistema documentale diventa coerente:

PEI-A → Informativa

↓

PEI-B → chi può partecipare e con quale titolo

↓

PEI-C → come deve comportarsi chi tratta i dati

↓

PEI-D → come viene gestito l'accesso digitale

↓

PEI-E → come possono essere comunicati/trasmessi i dati

↓

PEI-F → cosa fare se qualcosa va storto

Questa serie di procedure costruisce una vera **catena di accountability documentabile, che fornisce alla Scuola e agli operatori un supporto prezioso per corretta per la procedura relativa al PEI digitalizzato**

SEZIONE A: PROCEDURA DI COSTITUZIONE, AUTORIZZAZIONE E GESTIONE DEI COMPONENTI DEL GLO

a 1. COSTITUZIONE DEL GLO

Per ciascun alunno con accertata condizione di disabilità ai fini dell'inclusione scolastica è costituito il **Gruppo di Lavoro Operativo per l'Inclusione (GLO)**.

Il GLO opera per la definizione del PEI e per la verifica del processo di inclusione, compresa la proposta di quantificazione delle ore di sostegno e delle altre misure di sostegno.

La composizione del GLO deve essere conforme alla normativa vigente e comprende, secondo le specifiche condizioni previste dalla legge:

- il team dei docenti contitolari o il consiglio di classe;
- il dirigente scolastico o un suo delegato;
- i genitori dell'alunno o chi esercita la responsabilità genitoriale;
- lo studente, quando previsto e secondo il principio di autodeterminazione;
- le figure professionali specifiche interne ed esterne alla scuola che interagiscono con la classe e/o con l'alunno;
- il necessario supporto dell'unità di valutazione multidisciplinare;
- gli ulteriori soggetti la cui partecipazione sia prevista dalla normativa.

La composizione deve essere formalizzata dall'Istituto secondo le modalità organizzative previste dalla disciplina vigente.

La base normativa primaria è rappresentata dall'art. 9, comma 10 e seguenti, del D.Lgs. 66/2017. [Normattiva](#)

a 2. REGISTRO INTERNO DEI COMPONENTI DEL GLO

La scuola deve mantenere una **evidenza documentale interna della composizione di ciascun GLO**.

Per ciascun alunno devono essere registrate, almeno ove pertinenti:

1. anno scolastico;
2. identificativo interno dell'alunno;
3. classe;
4. composizione del GLO;
5. nominativo del componente;
6. ruolo ricoperto;
7. appartenenza all'Istituto o soggetto esterno;
8. eventuale qualifica professionale;
9. titolo che legittima la partecipazione;
10. data di inserimento nel GLO;
11. eventuale abilitazione/accesso SIDI;
12. profilo di accesso attribuito;
13. data di cessazione;
14. eventuali modifiche intervenute.

Il registro è un documento **riservato**.

Non deve essere pubblicato sul sito, sull'Albo online, in Amministrazione Trasparente, nel registro elettronico accessibile ad altri genitori o mediante altri canali accessibili a soggetti non legittimati.

a 3. PRINCIPIO DI AUTORIZZAZIONE INDIVIDUALE

Personale interno

Il personale scolastico che tratta dati personali nell'ambito delle proprie funzioni deve essere previamente individuato e autorizzato al trattamento secondo l'organizzazione privacy dell'Istituto.

L'autorizzazione deve essere:

- personale;
- nominativa;
- coerente con il ruolo;
- limitata ai dati necessari;
- limitata alle finalità istituzionali;
- coerente con le effettive funzioni svolte;
- soggetta a revoca o modifica.

L'autorizzazione non attribuisce un diritto generale di accesso alla documentazione degli alunni con disabilità.

Componenti esterni del GLO

La scuola **non deve qualificare automaticamente come “autorizzati dal Titolare” tutti i componenti esterni del GLO**.

Per ciascun soggetto esterno deve essere verificato:

- il titolo che ne legittima la partecipazione;
- il ruolo ricoperto;
- il rapporto con l'alunno;
- il rapporto con la scuola;
- la natura del trattamento effettuato;
- l'eventuale appartenenza ad altra amministrazione, ente o struttura;
- il relativo regime di responsabilità sul trattamento.

L'accesso deve essere limitato alle informazioni necessarie alla partecipazione al GLO e alle funzioni effettivamente esercitate.

a 4. CESSAZIONE DELL'AUTORIZZAZIONE O DELL'ACCESSO

L'accesso deve essere immediatamente riesaminato quando:

- il componente cessa di appartenere al GLO;
- viene sostituito;
- cambia ruolo;
- cessa il rapporto con l'Istituto;
- l'alunno cambia classe o istituzione scolastica;
- viene modificata la composizione del GLO;
- viene meno il presupposto che legittimava la partecipazione;
- viene rilevato un utilizzo improprio dell'accesso;
- si verifica un incidente di sicurezza.

La cessazione deve essere documentata.

Nel caso di accesso SIDI, la scuola deve verificare che l'abilitazione venga conseguentemente aggiornata o revocata secondo le funzionalità previste dal sistema.

a 5. ACCESSO DEI SOGGETTI ESTERNI

L'accesso di specialisti, professionisti o altri soggetti esterni deve essere preceduto dalla verifica del titolo che ne legittima la partecipazione.

Non è sufficiente la mera conoscenza personale dell'alunno o una richiesta informale.

Il soggetto deve essere identificabile e deve risultare:

- chi è;
- quale ruolo ricopre;
- perché partecipa;
- quale documentazione può conoscere;
- per quale periodo;
- quali sono i limiti del suo accesso.

La partecipazione al GLO non comporta un diritto generalizzato di acquisire o conservare autonomamente tutta la documentazione scolastica dell'alunno.

EVIDENZE DA CONSERVARE

L'Istituto deve poter dimostrare, in caso di verifica:

- decreto/atto di costituzione del GLO;
- composizione aggiornata;
- evidenza delle modifiche;
- autorizzazioni del personale interno;
- evidenza delle abilitazioni SIDI;
- eventuali revoche;
- eventuali comunicazioni ai componenti;
- documentazione relativa ai soggetti esterni.

SEZIONE B: ISTRUZIONI AGLI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI NELL'AMBITO DEL PEI E DEL GLO

b1. PRINCIPIO GENERALE

Il personale autorizzato al trattamento deve trattare i dati personali relativi al PEI e al GLO esclusivamente:

- nell'esercizio delle proprie funzioni;
- per finalità istituzionali;
- secondo le istruzioni ricevute;
- nei limiti delle proprie competenze;
- limitatamente ai dati necessari;
- nel rispetto del principio di riservatezza.

I dati relativi alla disabilità, alla salute e al PEI devono essere considerati **informazioni ad elevata sensibilità organizzativa e privacy**.

Il personale deve operare secondo i principi di:

- liceità;
- correttezza;
- trasparenza;

- minimizzazione;
- pertinenza;
- esattezza;
- riservatezza;
- sicurezza.

b2. DIVIETI SPECIFICI

È vietato:

1. utilizzare credenziali appartenenti ad altre persone;
2. condividere le proprie credenziali;
3. lasciare una sessione SIDI aperta e accessibile a soggetti non autorizzati;
4. inviare PEI o documentazione GLO mediante account personali;
5. utilizzare servizi cloud personali;
6. utilizzare WhatsApp o altri sistemi di messaggistica personale per trasmettere PEI o documentazione sanitaria;
7. fotografare PEI, verbali o documentazione sanitaria con dispositivi personali;
8. conservare copie non necessarie su dispositivi personali;
9. lasciare documenti cartacei incustoditi;
10. comunicare informazioni relative alla disabilità ad altri genitori;
11. inserire informazioni relative al PEI in comunicazioni collettive;
12. pubblicare convocazioni GLO;
13. pubblicare PEI o estratti del PEI;
14. comunicare a terzi l'esistenza di un PEI quando non necessario;
15. utilizzare iniziali ritenendo automaticamente che ciò renda anonima una comunicazione.

Quest'ultimo punto è particolarmente importante: il Garante ha espressamente rilevato che la sostituzione del nome con le iniziali non garantisce l'anonimizzazione quando il contesto consente comunque di identificare l'alunno. [Garante Privacy](#)

b3. PRINCIPIO DI RISERVATEZZA

Sono soggette a particolare riservatezza:

- diagnosi;
- certificazioni;
- informazioni sulla disabilità;
- dati relativi alla salute;
- PEI;
- verbali GLO;
- convocazioni GLO;
- informazioni relative agli interventi terapeutici;
- informazioni relative al contesto familiare quando pertinenti al PEI;
- informazioni relative alle esigenze assistenziali;
- credenziali e informazioni di accesso.

Il personale non deve discutere tali informazioni:

- nei corridoi;
- in presenza di altri genitori;
- nelle chat di classe;
- nelle comunicazioni collettive;
- attraverso social network;
- mediante strumenti non autorizzati.

Il Garante ha stabilito che persino la **convocazione del GLO**, per il suo stesso significato, può costituire informazione relativa allo stato di salute dell'alunno. [Garante Privacy](#)

b4. OBBLIGO DI SEGNALAZIONE

Il personale autorizzato deve segnalare **immediatamente** al dirigente scolastico e ai soggetti individuati nella procedura Data Breach dell'Istituto:

- invio errato;
- accesso non autorizzato;

- perdita di documentazione;
- furto di dispositivi;
- pubblicazione accidentale;
- destinatario errato;
- compromissione delle credenziali;
- visualizzazione da parte di soggetti non autorizzati;
- accesso ancora attivo di un ex componente del GLO;
- trasmissione attraverso canali non autorizzati.

La segnalazione deve avvenire anche quando l'evento sia stato immediatamente corretto.

Non è compito del dipendente stabilire autonomamente che l'evento “non è grave”.

SEZIONE C: PROCEDURA PER LA GESTIONE DEGLI ACCESSI AL PEI DIGITALE

c1. PRINCIPIO DEL MINIMO PRIVILEGIO

L'accesso deve essere attribuito secondo il principio del **minimo privilegio**.

Ogni soggetto deve poter accedere esclusivamente:

- agli alunni per i quali è legittimato;
- alle informazioni necessarie;
- alle funzionalità necessarie;
- per il periodo necessario.

Non deve essere attribuito un accesso generalizzato ai PEI di tutti gli alunni con disabilità.

c2. PROCEDURA DI ABILITAZIONE

L'abilitazione deve seguire almeno le seguenti fasi:

Fase 1 – Costituzione del GLO

La scuola definisce formalmente la composizione del GLO.

Fase 2 – Identificazione

Viene verificata l'identità del soggetto e il relativo ruolo.

Fase 3 – Verifica del titolo

Viene verificato il titolo che legittima la partecipazione.

Fase 4 – Definizione del livello di accesso

Viene individuata la funzione effettivamente necessaria:

- visualizzazione;
- gestione/modifica;
- sottoscrizione;
- altre funzionalità previste dal sistema.

Fase 5 – Abilitazione

La segreteria procede all'abilitazione secondo le funzionalità SIDI.

Fase 6 – Verifica

La scuola verifica che l'accesso attribuito corrisponda al ruolo effettivo.

Fase 7 – Registrazione

L'attività deve essere documentabile attraverso l'evidenza interna della composizione e delle abilitazioni.

Il modello ministeriale prevede espressamente l'accesso dei componenti del GLO al sistema SIDI tramite registrazione e apposite credenziali. [Istruzione](#)

c3. CREDENZIALI

Le credenziali sono:

- personali;
- non cedibili;
- non condivisibili;
- utilizzabili esclusivamente dal titolare;
- protette da adeguate misure di sicurezza.

È vietato:

- comunicare la password;
- utilizzare quella di un collega;
- conservare password in luoghi accessibili;

- lasciare la sessione aperta;
- consentire ad altri soggetti di utilizzare il proprio account.

L'autenticazione deve avvenire mediante le modalità previste dal sistema ministeriale.

c4. ACCESSO FISICO

Quando il PEI viene visualizzato o trattato presso la scuola:

- lo schermo deve essere protetto da visualizzazioni indebite;
 - i documenti cartacei non devono essere lasciati incustoditi;
 - le stampe devono essere limitate alle effettive necessità;
 - le copie devono essere custodite;
 - le copie non più necessarie devono essere eliminate secondo le procedure di sicurezza dell'Istituto.
-

c5. ACCESSO DA REMOTO

L'accesso da remoto è consentito esclusivamente mediante gli strumenti e le modalità autorizzate.

È vietato utilizzare:

- computer pubblici;
- dispositivi di terzi non adeguatamente protetti;
- account personali per la condivisione;
- cloud personali;
- strumenti di messaggistica non autorizzati.

L'eventuale partecipazione telematica alle riunioni GLO deve avvenire assicurando che soggetti estranei non possano ascoltare o visualizzare le informazioni trattate.

c6. VERIFICA PERIODICA

La scuola deve effettuare una verifica degli accessi:

- all'inizio dell'anno scolastico;
- ad ogni variazione del GLO;
- in caso di sostituzione di un componente;
- in caso di trasferimento;
- alla cessazione del rapporto;
- quando viene modificato il ruolo;
- in caso di incidente di sicurezza.

La verifica deve produrre un'evidenza documentale.

SEZIONE D: PROCEDURA PER LA COMUNICAZIONE, TRASMISSIONE E PUBBLICAZIONE DEL PEI E DELLE INFORMAZIONI RELATIVE AL GLO

d1. REGOLA GENERALE

Le informazioni relative al GLO e al PEI devono essere comunicate esclusivamente ai soggetti che hanno titolo a conoscerle.

Il principio organizzativo è:

la conoscenza del dato deve essere limitata ai soggetti legittimati e alle informazioni necessarie per lo svolgimento della specifica funzione.

Il PEI, la documentazione sanitaria e le informazioni relative alla disabilità **non devono essere pubblicati mediante strumenti destinati alla generalità degli utenti.**

Sono pertanto vietate, salvo specifica diversa base giuridica prevista dalla legge e comunque previa verifica privacy:

- pubblicazione sul sito web;
- Albo online;
- Amministrazione Trasparente;
- homepage;
- social network;
- circolari pubbliche;
- registro elettronico accessibile a soggetti non legittimati;
- bacheche elettroniche generali;
- mailing list di classe;

- gruppi WhatsApp;
- altri strumenti collettivi.

Il Garante ha recentemente sanzionato la pubblicazione sul sito scolastico delle convocazioni GLO relative a 51 alunni, ritenendo tale pubblicazione una diffusione di dati relativi alla salute. [Garante Privacy](#)

d2. CONVOCAZIONI GLO

La convocazione deve essere trasmessa **direttamente ai soggetti legittimati**.

La comunicazione deve essere predisposta verificando:

1. destinatario;
2. indirizzo;
3. oggetto;
4. contenuto;
5. eventuali allegati;
6. legittimazione del destinatario.

La convocazione non deve essere inserita in:

- circolari generali;
- bacheche accessibili a tutti i genitori;
- sito pubblico;
- homepage;
- registro elettronico accessibile a tutti i genitori della classe quando questi non siano legittimati alla conoscenza del dato.

Il Garante ha espressamente affermato che la convocazione GLO rappresenta di per sé un'informazione relativa allo stato di salute dell'alunno. [Garante Privacy](#)

d3. COMUNICAZIONI SCUOLA-FAMIGLIA

Le comunicazioni relative al PEI devono essere effettuate direttamente agli esercenti la responsabilità genitoriale o agli altri soggetti legittimati.

Prima dell'invio deve essere verificato:

- corretto destinatario;
- corretto indirizzo;
- eventuale presenza di altri destinatari in copia;
- contenuto;
- allegati;
- necessità della comunicazione.

È vietato utilizzare liste di distribuzione collettive quando il contenuto consenta di desumere la condizione di disabilità di uno studente.

d4. TRASMISSIONE DELLA DOCUMENTAZIONE

La documentazione deve essere trasmessa attraverso strumenti istituzionali e secondo modalità che assicurino:

- autenticazione;
- riservatezza;
- integrità;
- corretta identificazione del destinatario;
- tracciabilità ove disponibile;
- minimizzazione.

Prima dell'invio l'operatore deve effettuare un controllo **“destinatario-documento-allegato”**.

In particolare deve verificare:

A chi sto inviando?

Che cosa sto inviando?

Perché lo sto inviando?

Il destinatario ha titolo a riceverlo?

d5. REGOLA FONDAMENTALE

La presenza di un soggetto nella comunità scolastica non attribuisce automaticamente il diritto di conoscere l'esistenza o il contenuto del PEI.

La conoscenza deve essere collegata alla funzione concretamente esercitata.

Particolare attenzione deve essere posta anche alle iniziali dell'alunno: la sostituzione del nome con le sole iniziali non rende automaticamente anonimo il dato quando il contesto consente l'identificazione.

SEZIONE E: PROCEDURA DI GESTIONE DEGLI INCIDENTI E DEI DATA BREACH RELATIVI AL PEI E AL GLO

e1. DEFINIZIONE

Ai fini della presente procedura, costituisce potenziale incidente di sicurezza qualsiasi evento che comporti, anche solo potenzialmente:

- accesso non autorizzato;
- comunicazione non autorizzata;
- perdita;
- distruzione;
- alterazione;
- indisponibilità;
- divulgazione;
- pubblicazione;
- sottrazione;
- compromissione di dati personali relativi al PEI/GLO.

Sono inclusi, a titolo esemplificativo:

- invio della convocazione GLO al genitore sbagliato;
- pubblicazione sul registro elettronico con accesso a soggetti non legittimati;
- pubblicazione sul sito;
- invio di un PEI a un destinatario errato;
- accesso SIDI da parte di un soggetto non più legittimato;
- furto di un dispositivo contenente documentazione;
- perdita di una copia cartacea;
- compromissione delle credenziali.

e2. ESEMPIO PARTICOLARMENTE GRAVE

Costituisce evento di particolare gravità:

la pubblicazione o comunicazione a soggetti non legittimati di una convocazione GLO, di un PEI o di informazioni che consentano di desumere la condizione di disabilità dell'alunno.

Il Garante ha qualificato la semplice convocazione GLO come informazione relativa allo stato di salute.

[Garante Privacy](#)

Sono stati inoltre rilevati casi di:

- invio errato della convocazione GLO;
- pubblicazione della convocazione sul sito web;
- pubblicazione di documentazione PEI a soggetti non legittimati.

e3. OBBLIGO DI SEGNALAZIONE IMMEDIATA

Chiunque venga a conoscenza dell'incidente deve segnalarlo **immediatamente** al Dirigente scolastico e ai soggetti individuati nella procedura generale di gestione delle violazioni dei dati personali.

Il DPO deve essere coinvolto tempestivamente nella valutazione.

Il dipendente non deve attendere di conoscere:

- la gravità dell'evento;
- il numero di persone coinvolte;
- se esista effettivamente un Data Breach;
- se sia necessaria una notifica al Garante.

La valutazione è di competenza dell'organizzazione secondo la procedura Data Breach.

e4. CONTENIMENTO IMMEDIATO

Una volta rilevato l'evento, devono essere adottate, secondo il caso concreto, misure di contenimento quali:

- rimozione immediata di una pubblicazione;

- disabilitazione del link;
- revoca dell'accesso;
- blocco dell'account;
- modifica delle credenziali compromesse;
- recupero del documento;
- richiesta di cancellazione al destinatario errato;
- verifica dei soggetti che hanno avuto accesso;
- acquisizione dei log disponibili;
- conservazione delle evidenze;
- blocco di ulteriori trasmissioni.

La rimozione immediata del documento **non elimina l'obbligo di valutare e documentare l'incidente**.

e5. VALUTAZIONE DEL DATA BREACH

La valutazione deve considerare almeno:

Natura dei dati

- dati identificativi;
- dati relativi alla salute;
- dati relativi alla disabilità;
- dati relativi a minori;
- dati familiari;
- PEI;
- verbali GLO.

Natura degli interessati

Particolare attenzione deve essere posta alla presenza di **minori**, per i quali il GDPR riconosce una specifica esigenza di protezione. [Garante Privacy](#)

Portata dell'evento

- numero degli interessati;
- numero dei destinatari;
- durata dell'esposizione;
- possibilità di ulteriore diffusione;
- possibilità di copia o download.

Conseguenze

Devono essere valutati i possibili rischi per gli interessati, compresi:

- discriminazione;
- stigmatizzazione;
- pregiudizio personale;
- lesione della riservatezza;
- perdita di controllo sui dati;
- danni derivanti dalla diffusione della condizione di disabilità.

Misure adottate

Devono essere valutati:

- tempestività del contenimento;
 - recuperabilità del documento;
 - possibilità di cancellazione;
 - numero effettivo dei soggetti che hanno avuto accesso;
 - efficacia delle misure adottate.
-

e6. DOCUMENTAZIONE E DECISIONE

Ogni potenziale Data Breach deve essere documentato.

La documentazione deve contenere almeno:

1. data e ora dell'evento;
2. data e ora della rilevazione;
3. soggetto che ha rilevato l'evento;
4. descrizione dell'incidente;
5. sistema/documento interessato;
6. categorie di dati coinvolti;

7. categorie di interessati;
8. destinatari o soggetti che potrebbero aver avuto accesso;
9. numero stimato degli interessati;
10. misure di contenimento;
11. valutazione del rischio;
12. valutazione della probabilità e gravità;
13. eventuale decisione di notificare il Garante;
14. eventuale decisione di comunicare la violazione agli interessati;
15. motivazione della decisione;
16. misure correttive;
17. misure preventive;
18. coinvolgimento del DPO;
19. chiusura dell'incidente.

La documentazione deve essere conservata in modo da consentire al Titolare di dimostrare la conformità agli obblighi del GDPR.

IL DIRIGENTE SCOLASTICO

Dott.ssa Michela Pirrò

Firma autografa sostituita a mezzo stampa ex
art.3, c.2 D.Lgs n. 39/93

