



ISTITUTO COMPRENSIVO EX S.M. "G. PASCOLI"

Via Parini, 1 - 75100 MATERA

Cod. Ministeriale: MTIC82700A – E-Mail: mtic82700a@istruzione.it Pec: mtic82700a@pec.istruzione.it

C.F.:93051600778 - Codice Univoco Ufficio: UF0G7C

Sito: www.icpascolimatera.it – telefono: 0835.386254 – Fax.0835.264648

LINEE GUIDA OPERATIVE

PER LA PREVENZIONE DELLA DIFFUSIONE DI DATI PERSONALI – GLO, PEI E PDP

IST. COMP. EX S.M. "G. PASCOLI" - MATERA Prot. 0006048 del 16/04/2026 I-4 (Uscita)
--

Premessa

A seguito dell'episodio verificatosi, relativo alla pubblicazione non corretta di una convocazione del GLO sulla bacheca del registro elettronico, l'Istituto Scolastico ha ritenuto necessario intervenire non solo sul piano tecnico, ma anche organizzativo e culturale.

L'obiettivo di queste linee guida non è quello di irrigidire l'attività amministrativa e didattica, ma di accompagnarla con regole chiare e sostenibili, che permettano di evitare errori, soprattutto in contesti delicati come quelli che riguardano gli alunni con bisogni educativi speciali.

1. Un principio da cui partire: non tutto ciò che è comunicazione è pubblicazione

Uno degli aspetti che l'episodio ha messo in evidenza è la tendenza, spesso inconsapevole, a utilizzare la bacheca digitale come strumento "generico" di comunicazione.

In realtà, è necessario distinguere:

- la comunicazione mirata, rivolta a soggetti determinati (docenti, famiglia, ASL)
- dalla pubblicazione, che comporta una potenziale diffusione dei dati.

Nel caso di documenti come:

- convocazioni GLO
- PEI
- PDP
- situazioni BES o disabilità

non siamo mai di fronte a comunicazioni “generiche”, **ma sempre a informazioni ad altissima riservatezza**, che non devono essere rese accessibili a soggetti diversi da quelli strettamente coinvolti.

2. Gestione delle convocazioni GLO: regola di base

Le convocazioni del GLO, per loro natura, contengono informazioni che possono rivelare indirettamente dati sulla salute dell'alunno/a.

Per questo motivo:

- non devono mai essere pubblicate in bacheca visibile alla classe o alle famiglie
- devono essere inviate esclusivamente:
 - ai docenti interessati
 - alla famiglia
 - agli operatori esterni autorizzati
 - utilizzando strumenti che consentano una selezione puntuale dei destinatari.

3. Introduzione di una procedura strutturata: il sistema dei codici per PEI e PDP

Per rafforzare la tutela dei dati degli alunni più esposti, l'Istituto Scolastico introduce una misura organizzativa **stabile e obbligatoria**.

3.1 Assegnazione del codice identificativo

Per ogni alunno:

1. con PEI (Piano Educativo Individualizzato)
2. con PDP (Piano Didattico Personalizzato)

il Consiglio di classe (o team docenti) è tenuto ad assegnare un codice identificativo univoco.

Il codice:

- deve essere deliberato in sede collegiale;
- deve essere riportato nei verbali interni;
- deve essere utilizzato in tutte le comunicazioni non strettamente individuali.

Esempio:

“ALUNNO PEI – COD. 3C/PEI/01”

“ALUNNO PDP – COD. 2A/PDP/02”

3.2 Utilizzo del codice nelle comunicazioni

A partire dall’assegnazione:

- tutte le comunicazioni interne, circolari, convocazioni e documenti digitali devono riportare solo il codice;
- il nominativo completo deve essere utilizzato solo nei canali diretti e riservati.

Questo consente, anche in caso di errore umano (es. pubblicazione errata), di ridurre significativamente il rischio di identificazione dell’alunno/a.

3.3 Custodia della chiave di corrispondenza

La corrispondenza tra:

- codice identificativo
- nominativo dell’alunno

deve essere:

- conservata in modo separato

accessibile solo a:

1. Dirigente scolastico;
2. docenti del consiglio di classe;
3. personale autorizzato.

4. Pseudonimizzazione come regola operativa

Accanto al sistema dei codici, si introduce una regola generale:

ogni volta che un documento non richiede l’identificazione diretta dell’alunno, si deve ricorrere a:

- codici identificativi
- diciture generiche (“alunno interessato”, “studente della classe...”)

Questo approccio consente di lavorare in modo più sicuro senza compromettere l’efficacia dell’azione didattica e amministrativa.

5. Controllo prima della pubblicazione: fermarsi un attimo

Un altro elemento emerso è la velocità operativa con cui vengono gestite le comunicazioni digitali.

Per questo motivo si introduce una regola semplice ma fondamentale:

prima di pubblicare, bisogna fermarsi e verificare tre cose:

- a. Chi vedrà questo documento?
- b. Contiene dati personali o sensibili?
- c. Esiste un modo più sicuro per inviarlo?

Quando anche solo una di queste domande genera un dubbio, la pubblicazione deve essere evitata.

6. Doppio controllo nei casi più delicati

Per documenti che riguardano:

- GLO
- PEI
- PDP
- situazioni BES

si introduce una prassi di verifica preventiva:

1. un operatore inserisce il documento
2. un secondo operatore verifica visibilità e contenuto

Non si tratta di appesantire il lavoro, ma di evitare errori che possono avere conseguenze rilevanti.

7. Cosa fare in caso di errore

Nel caso in cui si verifichi una pubblicazione non corretta:

- il documento deve essere rimosso immediatamente;
- deve essere informato con tempestività il Dirigente Scolastico
- deve essere coinvolto il DPO.

È importante che queste situazioni vengano gestite con tempestività e trasparenza, senza timore, perché è proprio dalla gestione corretta dell'errore che si misura l'affidabilità dell'Istituto Scolastico.

8. Una responsabilità condivisa

La protezione dei dati non è un adempimento formale, ma una responsabilità che riguarda tutti.

Nel contesto scolastico, questo assume un valore ancora più forte, perché:

- a. i soggetti coinvolti sono minori;
- b. spesso si tratta di situazioni di fragilità.

Per questo motivo, ogni attenzione in più non è un eccesso di prudenza, ma una forma di tutela concreta della dignità degli studenti.

9 Gestione dei fascicoli cartacei e degli archivi

Accanto alla gestione dei flussi digitali, l'Istituto Scolastico richiama l'attenzione sulla corretta gestione dei fascicoli cartacei contenenti dati personali, con particolare riferimento alla documentazione relativa a GLO, PEI, PDP e situazioni riconducibili a bisogni educativi speciali.

Tali documenti, per loro natura, contengono informazioni ad elevato livello di riservatezza e devono essere trattati con modalità idonee a garantirne la protezione anche in formato analogico.

In particolare:

- i fascicoli devono essere custoditi in armadi chiusi a chiave, ubicati in locali non accessibili al pubblico;
- l'accesso deve essere consentito esclusivamente al personale autorizzato, sulla base delle funzioni svolte;
- è fatto divieto di lasciare documenti contenenti dati personali incustoditi su scrivanie o in ambienti accessibili a terzi;
- la consultazione dei fascicoli deve avvenire in modo tale da evitare la visione da parte di soggetti non legittimati;
- eventuali copie devono essere limitate allo stretto necessario e distrutte con modalità idonee (es. distruggidocumenti) quando non più utili.

Particolare attenzione deve essere posta nella gestione dei momenti operativi (riunioni, GLO, colloqui con le famiglie), durante i quali i documenti non devono essere lasciati esposti o accessibili a soggetti diversi da quelli coinvolti.

La gestione dei fascicoli cartacei si inserisce nel più ampio sistema di protezione dei dati adottato dall'Istituto, in coerenza con i principi di integrità e riservatezza di cui all'art. 5 del Regolamento (UE) 2016/679.

10. Accesso ai locali e gestione degli archivi

La protezione dei dati personali non riguarda esclusivamente i sistemi informatici, ma anche gli spazi fisici in cui i dati vengono trattati e conservati.

Per questo motivo, l'Istituto adotta misure organizzative volte a limitare l'accesso ai locali in cui sono presenti dati personali, in particolare:

- uffici di segreteria
- archivi cartacei
- stanze utilizzate per riunioni riservate (es. GLO)

L'accesso a tali ambienti deve essere consentito esclusivamente al personale autorizzato, evitando la presenza non controllata di soggetti esterni o non coinvolti nelle attività.

Durante l'orario di apertura al pubblico, il personale è tenuto a prestare particolare attenzione affinché documenti o informazioni non siano visibili o accessibili a terzi.

11. Regola della “scrivania pulita” (clean desk)

Al fine di prevenire accessi indebiti o anche solo visioni accidentali di dati personali, viene introdotta una prassi organizzativa semplice ma efficace.

Al termine delle attività lavorative, nonché durante momenti di assenza dalla postazione (anche temporanea), il personale è tenuto a:

- non lasciare documenti contenenti dati personali esposti sulla scrivania;
- riporre i fascicoli in armadi o cassetti chiusi;
- evitare la presenza di elenchi, registri o appunti contenenti dati personali in vista;
- bloccare il computer o il dispositivo utilizzato.

Questa prassi si applica con particolare rigore ai documenti relativi a GLO, PEI, PDP e situazioni di fragilità.

12. Utilizzo di dispositivi rimovibili e protezione dei dati (USB, hard disk esterni)

L'utilizzo di dispositivi di archiviazione rimovibili (chiavette USB, hard disk esterni, ecc.) deve essere limitato ai soli casi strettamente necessari.

Qualora il loro utilizzo si renda indispensabile:

- i dispositivi devono essere protetti mediante sistemi di cifratura (crittografia) o password;
- i dati contenuti devono essere limitati allo stretto necessario;
- è vietato l'utilizzo di dispositivi personali non autorizzati;

- è fatto divieto di lasciare incustoditi i dispositivi contenenti dati personali;
- i dati devono essere cancellati una volta cessata la finalità per cui sono stati trasferiti.

In particolare, è fortemente sconsigliato il trasferimento su dispositivi rimovibili di documenti contenenti dati appartenenti a categorie particolari, salvo casi eccezionali adeguatamente motivati.

13. Modalità corrette di utilizzo della posta elettronica per comunicazioni contenenti dati personali

La posta elettronica rappresenta uno strumento fondamentale di lavoro, ma deve essere utilizzata con particolare attenzione quando si trattano dati personali.

In caso di comunicazioni contenenti dati personali, e in particolare dati relativi a:

- GLO
- PEI
- PDP
- disabilità o bisogni educativi speciali

il personale è tenuto a:

1. verificare con attenzione i destinatari prima dell'invio;
2. utilizzare preferibilmente indirizzi istituzionali e nominativi;
3. evitare invii multipli a destinatari non strettamente necessari;
4. utilizzare, ove possibile, campi di copia nascosta (CCN) per evitare la visibilità degli indirizzi email tra destinatari non collegati tra loro;
5. evitare l'inserimento di dati sensibili nel corpo della mail quando non strettamente necessario, privilegiando allegati protetti;
6. proteggere gli allegati contenenti dati particolari tramite password, da trasmettere con canale separato.

È inoltre fatto divieto di utilizzare account personali per la trasmissione di dati personali relativi agli alunni/e.

14. Conclusione

L'Istituto, attraverso queste linee guida, intende:

- trasformare un episodio critico in un'occasione di miglioramento;
- rafforzare le proprie procedure interne;
- garantire una gestione sempre più attenta e consapevole dei dati personali.

L'introduzione del sistema dei codici per PEI e PDP rappresenta, in questo senso, una misura concreta e strutturale, capace di prevenire il ripetersi di situazioni analoghe.

L'Istituto si impegna a garantire attività periodiche di formazione e aggiornamento del personale in materia di protezione dei dati personali, con particolare riferimento ai trattamenti riguardanti minori e categorie particolari di dati.

Il rispetto delle presenti linee guida costituisce parte integrante degli obblighi di servizio del personale ed è oggetto di vigilanza da parte del Dirigente scolastico, anche ai fini della responsabilità disciplinare in caso di violazioni.

Dirigente Scolastico

Prof.ssa Caterina POLICARO

Documento firmato digitalmente
ai sensi del codice dell'Amministrazione digitale e normativa connessa