Ministero dell'Istruzione e del Merito
ISTITUTO COMPRENSIVO STATALE DI BADESI
Via L'Ua Bianca, 8 – Tel/Fax 079/684042 – 07053 BADESI (SS)
e-mail: ssic80800g@istruzione.it - Pec: ssic80800g@pec.istruzione.it - sito web: www.icbadesi.edu.it C.M **ssic80800g**- C.F **91015280901**- Codice IPA**: istsc_ssic80800g** - Codice Univoco: **UFEB0V**

Circ. n°31 Badesi, 12 ottobre 2026

Al personale docente
Al personale ATA
Ai coordinatori dei consigli di classe
Al DSGA
Agli atti

Oggetto: Disposizioni sulla riservatezza dei documenti e delle comunicazioni contenenti dati particolari degli alunni. Strumenti di condivisione, cifratura dei documenti e gestione delle password.

Nell'attività quotidiana della scuola circolano numerosi documenti che contengono informazioni delicate sugli alunni e sulle loro famiglie: piani educativi e didattici personalizzati, diagnosi e certificazioni, relazioni, verbali, resoconti di colloqui. La loro condivisione fra i componenti del consiglio di classe è indispensabile, ma l'esperienza dimostra che un errore nella scelta dei destinatari di una mail, un caricamento nell'area sbagliata del Registro Elettronico o lo smarrimento di una chiavetta USB possono esporre queste informazioni a persone non autorizzate, con conseguenze gravi per gli alunni interessati e per l'Istituto.

Con la presente disposizione si stabiliscono le regole che tutto il personale è tenuto a osservare per ridurre il rischio di tali incidenti e per contenerne le conseguenze, in primo luogo mediante la cifratura dei documenti.

IL DIRIGENTE SCOLASTICO

VISTI gli artt. 5, 9, 29, 32, 33 e 34 del Regolamento (UE) 2016/679 (GDPR);

VISTO l'art. 2-quaterdecies del D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali);

VISTE le istruzioni già impartite al personale autorizzato al trattamento dei dati personali;

VISTE le indicazioni fornite dal Responsabile della protezione dei dati con la nota VS_DPO 107/2026;

DISPONE

che tutto il personale osservi le seguenti regole nella condivisione e nella conservazione dei documenti e delle informazioni riservate.

Art. 1 – Documenti interessati

Le presenti disposizioni si applicano a tutti i documenti e le comunicazioni che contengono dati relativi alla salute, alla disabilità, ai bisogni educativi speciali o alla situazione personale e familiare degli alunni, e in particolare a:

- PEI, PDP, diagnosi, certificazioni e relazioni specialistiche;
- verbali del GLO e delle sedute del consiglio di classe contenenti informazioni riservate;
- segnalazioni ai servizi sociali o sanitari e relative comunicazioni;

Le stesse cautele si applicano ai documenti contenenti dati particolari relativi al personale.

Art. 2 – Strumenti di condivisione

I documenti di cui all'art. 1 possono essere condivisi esclusivamente con i seguenti strumenti, in ordine di preferenza:

a) **Registro Elettronico e piattaforme istituzionali** (solo Google Workspace), utilizzando le aree riservate ai soli destinatari autorizzati e verificando ogni volta l'area e i destinatari selezionati;

b) **posta elettronica istituzionale**, solo con il documento in allegato e cifrato;

È in ogni caso **vietato** utilizzare per la condivisione dei documenti e delle informazioni di cui all'art. 1:

– le applicazioni di messaggistica istantanea (ad esempio WhatsApp e Telegram), anche nei gruppi riservati ai docenti;

– le caselle di posta elettronica personali;

– gli spazi cloud personali;

– i servizi online di conversione o protezione dei documenti.

Art. 3 – Obbligo di cifratura

I documenti di cui all'art. 1 devono essere **cifrati prima di ogni condivisione o invio**, qualunque sia lo strumento utilizzato, con le funzioni descritte nelle schede operative allegate. In particolare:

- occorre utilizzare esclusivamente la funzione che impone una password di apertura, e non quelle che si limitano a impedire la modifica o la stampa;
- dopo la cifratura occorre verificare, riaprendo il file, che la password venga richiesta;
- il nome del file non deve contenere il nome o il cognome dell'alunno;
- le informazioni riservate non devono essere scritte nel testo dei messaggi di posta elettronica, ma in un documento allegato e cifrato;
- l'originale non cifrato va conservato esclusivamente negli spazi indicati dall'Istituto.

Art. 4 – Caratteristiche della password

La password utilizzata per la cifratura dei documenti e dei dispositivi è composta da **tre parole scelte a caso e senza legame fra loro, separate da due cifre anch'esse scelte a caso** (ad esempio del tipo tegola7limone3vento). Parole e cifre vanno scelte a caso e non inventate, ad esempio aprendo un libro a tre pagine diverse e prendendo da ciascuna la prima parola e l'ultima cifra del numero di pagina. La password non deve contenere nomi, classi, anni, date o riferimenti all'Istituto, né essere utilizzata per altri servizi.

La password **non deve mai essere** scritta nei verbali, nel Registro Elettronico, nelle piattaforme istituzionali o in file e note salvati sui dispositivi, né trasmessa insieme al documento che protegge.

Art. 5 – Gestione della password

a) **Consiglio di classe.** Per i documenti condivisi fra i componenti del consiglio di classe si utilizza una password unica, definita all'inizio dell'anno scolastico secondo l'art. 6, che può restare invariata per l'intero ciclo di studi della classe.

b) **Comunicazioni tra docenti.** Se tutti i destinatari sono componenti del medesimo consiglio di classe si utilizza la password del consiglio, che non va riportata nel messaggio. Se il destinatario non fa parte del consiglio si utilizza una password specifica, comunicata secondo la lettera c).

c) **Famiglie e destinatari esterni.** I documenti vanno trasmessi ai soli genitori dell'alunno interessato, con comunicazione individuale, preferendo quando possibile la consegna diretta. Il documento va cifrato con una password specifica, diversa da quella del consiglio di classe, comunicata attraverso un **canale separato** (a voce, per telefono o con un messaggio su un diverso mezzo di comunicazione).

Art. 6 – Compiti del coordinatore di classe

Il coordinatore di classe:

- nella prima seduta utile dell'anno scolastico fa definire al consiglio la password, che viene comunicata a voce ai soli componenti presenti;
- fa riportare a verbale esclusivamente la formula indicata di seguito, senza alcuna indicazione della password;
- comunica la password, di persona o per telefono, ai componenti assenti e ai docenti che entrano a far parte del consiglio nel corso del ciclo;
- promuove la sostituzione della password qualora vi sia motivo di ritenere che sia stata conosciuta da persone estranee al consiglio, informandone il Dirigente Scolastico.

> **Formula da riportare a verbale:** «Il consiglio di classe ha provveduto alla definizione della password per la cifratura dei documenti riservati, comunicata ai soli componenti e non riportata nel presente verbale.»

Art. 7 – Dispositivi personali e conservazione dei documenti

I documenti di cui all'art. 1 vanno conservati, di norma, negli spazi istituzionali messi a disposizione dall'Istituto. Il personale che li conservi, anche temporaneamente, su un computer personale deve cifrarne il disco oppure cifrare i singoli documenti, secondo le schede operative allegate. L'accesso al computer deve essere protetto da una password robusta, diversa da quelle utilizzate per altri servizi, e il blocco automatico dello schermo deve essere attivo. Le copie di lavoro non più necessarie vanno eliminate, comprese quelle presenti nella cartella dei download. Le chiavette USB eventualmente utilizzate devono essere cifrate per intero e, al termine del loro utilizzo, i documenti vi vanno cancellati.

Art. 8 – Disposizioni per il personale di segreteria

Il personale di segreteria applica le presenti disposizioni anche alla trasmissione di documenti contenenti dati particolari a soggetti esterni all'Istituto, quali aziende sanitarie, servizi sociali, enti locali, altre istituzioni scolastiche e autorità giudiziarie. Le modalità di trasmissione vanno **concordate preventivamente con ciascun ente**, a cura del DSGA o del Dirigente Scolastico, tenendo conto degli strumenti di cui l'ente dispone e dell'effettiva necessità di cifrare i documenti. Quando l'ente mette a disposizione una propria piattaforma di trasmissione, o quando lo scambio avviene mediante posta elettronica certificata fra indirizzi istituzionali predefiniti, la cifratura può non essere necessaria. Negli altri casi i documenti sono trasmessi cifrati, con password comunicata all'ente attraverso un canale separato. Le modalità concordate con ciascun ente sono annotate e comunicate al personale incaricato, così che vengano applicate in modo uniforme.

Il personale di segreteria non conserva documenti riservati sul desktop o su supporti rimovibili. Qualora all'avvio del computer compaia la richiesta di una chiave di ripristino, non tenta alcuna operazione e si rivolge all'amministratore di sistema.

Art. 9 – Segnalazione degli incidenti

Chiunque si accorga che un documento, anche cifrato, è stato caricato in un'area errata, inviato a un destinatario sbagliato o reso comunque accessibile a persone non autorizzate, o che un dispositivo contenente documenti dell'Istituto è stato smarrito o sottratto, deve **rimuovere immediatamente il contenuto, ove possibile, e informare senza ritardo il Dirigente Scolastico**, indicando che cosa è accaduto e quando, i documenti o dispositivi coinvolti, se erano cifrati e con quale tipo di password, senza riportarla. La segnalazione è dovuta anche quando l'errore sia stato corretto: spetta al Dirigente Scolastico, con il Responsabile della protezione dei dati, valutare l'evento entro le 72 ore previste dall'art. 33 del GDPR.

Art. 10 – Disposizioni finali

La presente disposizione costituisce **integrazione delle istruzioni impartite al personale autorizzato al trattamento** dei dati personali ai sensi dell'art. 29 del GDPR e dell'art. 2-quaterdecies del D.Lgs. 196/2003, ed è vincolante per tutto il personale a partire **dal 10 novembre 2026.** Le schede operative allegate ne costituiscono

parte integrante. I docenti fino a quella data potranno visionare, i documenti presso la segreteria, previo appuntamento con ufficio alunni.

La disposizione è pubblicata nell'area riservata del sito e nella bacheca del Registro Elettronico e trasmessa a tutto il personale. Il personale è tenuto a prenderne visione e a darne conferma secondo le modalità consuete.

Il Dirigente Scolastico
Dott.ssa Alessandra Pinna

Allegati: schede operative per la cifratura dei documenti