



Istituto Comprensivo Statale "A. Frank – Carradori"

Via Donati, 19 - 51100 Pistoia

Tel. 0573-367580 Tel. e Fax 0573-26784

e-mail: ptic82800a@istruzione.it PEC:ptic82800a@pec.istruzione.itwww.icsfrankcarradori.edu.it

Cod. fisc. 80008010474



I.C. "A. FRANK - CARRADORI"-PISTOIA
Prot. 0010594 del 19/10/2026
VII-5 (Uscita)

VADEMECUM PRIVACY PER I DOCENTI*Principali adempimenti e buone prassi per il trattamento dei dati personali*

Principio generale. Il docente tratta i dati personali degli alunni, delle famiglie e del personale esclusivamente per finalità istituzionali, nei limiti delle proprie funzioni e delle autorizzazioni ricevute dall'Istituto. Devono essere trattati solo i dati necessari, evitando comunicazioni, copie, condivisioni o conservazioni non indispensabili.

1. Registro elettronico

- Utilizzare esclusivamente le proprie credenziali; non comunicarle a colleghi, studenti o familiari e non lasciare sessioni aperte su dispositivi incustoditi.
- Verificare sempre classe, alunno e destinatari prima di inserire voti, note, assenze, annotazioni, allegati o comunicazioni.
- Usare le funzioni del registro secondo i profili autorizzativi: una bacheca visibile a famiglie/studenti non deve essere utilizzata per comunicazioni interne contenenti dati personali del personale o di singoli alunni.
- Evitare nelle annotazioni dettagli eccedenti o informazioni sanitarie non necessarie. Le note devono essere pertinenti, corrette e formulate con linguaggio professionale.
- Non esportare elenchi, voti o altri dati su dispositivi personali o servizi cloud non autorizzati dall'Istituto.

2. Dati particolari e situazioni delicate

- Dati relativi alla salute, disabilità, DSA/BES, convinzioni religiose e altre categorie particolari devono essere conosciuti e utilizzati solo quando necessario per le funzioni didattiche ed educative e nei limiti delle istruzioni dell'Istituto.
- PEI, PDP, certificazioni sanitarie e altra documentazione riservata non devono essere lasciati incustoditi, fotografati, inoltrati tramite chat personali o conservati su dispositivi/cloud non autorizzati.
- Non rendere identificabili in circolari, elenchi, presentazioni o comunicazioni collettive gli alunni interessati da disabilità, problemi di salute, diete sanitarie, provvedimenti disciplinari, bullismo o altre vicende delicate.
- Condividere le informazioni solo con i soggetti che hanno effettiva necessità di conoscerle.

3. Comunicazioni scuola-famiglia

- Utilizzare prioritariamente i canali istituzionali: registro elettronico, account e-mail istituzionale e altri strumenti approvati dalla scuola.
- Prima dell'invio verificare destinatari, allegati e visibilità della comunicazione. Prestare particolare attenzione a CC/CCN nelle e-mail collettive.
- Le comunicazioni riferite a un singolo alunno devono essere indirizzate esclusivamente ai soggetti legittimati; evitare informazioni personali nelle circolari rivolte alla generalità delle famiglie.
- Le chat personali o di gruppo non devono sostituire i canali istituzionali per comunicazioni ufficiali né essere utilizzate per condividere documenti o dati riservati.

4. Foto, video e registrazioni

- Foto, video e registrazioni realizzati dalla scuola devono avere una finalità istituzionale/didattica definita e rispettare le indicazioni e le informative adottate dall'Istituto.
- Non pubblicare autonomamente immagini o video degli alunni su profili social personali, gruppi WhatsApp, siti, blog o piattaforme non autorizzate.

- Prima di utilizzare immagini per finalità ulteriori rispetto all'attività didattica ordinaria (ad es. diffusione sul sito/social istituzionali), attenersi alle procedure e alle eventuali autorizzazioni previste dall'Istituto.
- Durante recite, gite ed eventi ricordare a studenti e famiglie che l'eventuale diffusione online di immagini deve rispettare i diritti delle persone riprese.

5. Documenti cartacei e digitali

- Non lasciare registri, verifiche, elenchi, PEI/PDP o documenti contenenti dati personali in luoghi accessibili a persone non autorizzate.
- Quando non più necessari, consegnare/archiviare i documenti secondo le procedure dell'Istituto; non smaltire documenti con dati personali nei normali cestini senza adeguata distruzione.
- Bloccare lo schermo quando ci si allontana dal dispositivo; evitare il salvataggio automatico di password su dispositivi condivisi.
- Non utilizzare chiavette USB, account personali, servizi personali o non autorizzati di archiviazione e condivisione di file online (es. cloud, Drive personali, Dropbox, WeTransfer o servizi analoghi) per archiviare o trasferire dati scolastici.

6. E-mail, phishing e sicurezza informatica

- Non aprire allegati o collegamenti sospetti e verificare con attenzione il mittente, soprattutto in messaggi che richiedono credenziali, pagamenti o azioni urgenti.
- Non inserire mai le credenziali scolastiche in pagine raggiunte da link dubbi. In caso di sospetto, contattare il referente tecnico/ufficio indicato dalla scuola.
- Utilizzare password robuste e, quando disponibile, l'autenticazione a più fattori. Non riutilizzare la password dell'account scolastico su servizi personali.

7. Piattaforme digitali e Intelligenza Artificiale

- Utilizzare esclusivamente piattaforme e applicazioni autorizzate dall'Istituto per attività che comportano trattamento di dati personali.
- Non inserire in strumenti di IA generativa non espressamente autorizzati nomi di studenti, elaborati identificabili, voti, profili individuali, dati sanitari, PEI/PDP, fotografie o altre informazioni riservate.
- Anche con strumenti autorizzati applicare il principio di minimizzazione: quando possibile usare dati anonimi, pseudonimizzati o esempi fittizi.
- Non affidare a sistemi automatizzati decisioni valutative o educative che richiedono il giudizio professionale del docente; verificare sempre gli output prodotti.

8. Data breach – cosa deve fare il docente

- È una possibile violazione anche: e-mail inviata al destinatario sbagliato; allegato errato; perdita/furto di PC o chiavetta; credenziali compromesse; accesso non autorizzato al registro; pubblicazione accidentale di dati; perdita o cancellazione di dati.
- NON attendere e NON valutare autonomamente se la violazione sia grave: informare immediatamente il Dirigente/ufficio o referente individuato dalla procedura interna, fornendo tutte le informazioni disponibili.
- Se possibile, adottare subito misure di contenimento senza cancellare elementi utili alla ricostruzione: ad es. chiedere al destinatario errato la cancellazione, revocare una condivisione, cambiare la password compromessa.
- Non effettuare direttamente la notifica al Garante e non comunicare autonomamente l'evento alle famiglie/interessati, salvo specifica istruzione: la valutazione e gli adempimenti competono al Titolare del trattamento.
- Annotare data/ora, dati coinvolti, destinatari, circostanze e misure già adottate e conservarne evidenza per la segnalazione interna.

9. Regole essenziali da ricordare

FARE	EVITARE
Usare i canali e gli strumenti autorizzati dalla scuola.	Usare account personali, chat o cloud privati per dati scolastici.
Trattare solo i dati necessari alla propria funzione.	Raccogliere o condividere informazioni "per comodità".

Controllare destinatari, allegati e permessi prima dell'invio.	Inviare elenchi o documenti riservati a gruppi non selezionati.
Segnalare immediatamente errori o incidenti.	Nascondere o rinviare la segnalazione di una possibile violazione.
Chiedere indicazioni al Dirigente/DPO in caso di dubbio.	Assumere iniziative autonome su trattamenti delicati.

Riferimenti essenziali: Regolamento (UE) 2016/679, in particolare artt. 5, 29, 32, 33 e 34; D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018; istruzioni e policy interne dell'Istituto; vademecum del Garante "La scuola a prova di privacy" (edizione aggiornata).

In caso di dubbio: non comunicare o diffondere il dato finché non è stata verificata la correttezza dell'operazione. Rivolgersi al Dirigente scolastico o al RPD/DPO [Ugo Antonino – mail info@egasoftservizi.it].

Data aggiornamento: [gg/mm/aaaa]

Il Dirigente Scolastico
Prof.ssa Margherita De Dominicis
*Firma sostituita a mezzo stampa ai sensi
dell'art.3, comma 2 del D.Lgs. N. 39/1993*