PROTOCOLLO
4603/U DEL 02/11/2026

STUDIO TECNICO LEGALE
CORBELLINI
Studio AGI.COM. S.r.l.

LETTERE CUMULATIVE

Egregio Dirigente Scolastico

quelle che seguono sono l'ultima tranche di lettere di autorizzazione.

Come già detto si tratta di lettere pensate per un operatore della scuola "standard" ossia che non svolga compiti speciali tali da rendere la sua figura specifica ai fini del trattamento di dati personali.

Troverà 5 lettere di autorizzazione : Docente, Collaboratore Scolastico, Membro della Commissione di formazione delle classi, Membro del Comitato di Valutazione e Addetto alla somministrazione di farmaci (Gli Istituti Superiori ne troveranno una quinta destinata agli Assistenti Tecnici). Potrà consegnarle agendo come ha fatto per le lettere nominative in quanto, al netto del fatto che manchi l'intestazione nominativa del destinatario, il loro "compito" è assolutamente lo stesso ossia quello di rammentare quali siano i trattamenti consentiti al fine di raggiungere le finalità proprie dei diversi incarichi.

Occorre precisare che, talvolta, se il lavoratore svolge qualche incarico particolare, non è necessario fornire anche la lettera cumulativa, poiché è sufficiente dare quella nominativa dedicata (p.es. la lettera cumulativa per il Collaboratore del Dirigente include già l'autorizzazione comune a tutti i docenti etc.).

-

-

-

-

-

-

-

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI (Art. 29 Regolamento UE 2016/679 - G.D.P.R.)

Titolare del trattamento dei dati:

ISTITUTO COMPRENSIVO "A. MANZONI"

Via Riccardo Lombardi, 12

20027 RESCALDINA (MI)

Autorizzato al trattamento dei dati:

DOCENTE

AUTORIZZAZIONE CUMULATIVA

Al fine di poter svolgere regolarmente i compiti inerenti ai seguenti incarichi a Lei assegnati:

A	**Docente**
B	**Membro del Gruppo di Lavoro Operativo (G.L.O.) istituito ai sensi dell'art. 15 della Legge 104/1992 come modificata dal Decreto Interministeriale 182 del 29/12/2020 (in caso di Sua designazione a membro del G.L.O.)**

appurato che detta attività comporta il trattamento di dati personali e considerato che Lei è in possesso di requisiti di esperienza e capacità tali da fornire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento dei dati, La informo che è autorizzata a trattare i seguenti dati:

	BASE DATI E LORO TIPOLOGIA	CATEGORIE DI INTERESSATI E FINALITA'
A	DATI INERENTI AGLI ALLIEVI [COMUNI E PARTICOLARI]	IL DOCENTE ACCEDE A DATI DI NATURA IDENTIFICATIVA E DI ANDAMENTO SCOLASTICO DI TUTTI GLI ALLIEVI DELLE CLASSI ASSEGNATE, SIA STABILMENTE CHE PERIODICAMENTE (SUPPLENZE). ACCEDE INOLTRE, POTENZIALMENTE, A DATI DI NATURA PARTICOLARE (SALUTE) E GIUDIZIARIA, NEL CASO DI ALLIEVI CON BISOGNI EDUCATIVI SPECIALI, SEMPRE LIMITATAMENTE AI COMPONENTI DELLE CLASSI ASSEGNATE.
B	DATI IDENTIFICATIVI [COMUNI] DATI INERENTI ALL'ANDAMENTO SCOLASTICO [COMUNI] DATI INERENTI ALLO STATO DI SALUTE [PARTICOLARI]	IL DOCENTE, IN AGGIUNTA ALLE AUTORIZZAZIONI AL TRATTAMENTO INERENTI AL PROPRIO RUOLO ORDINARIO, TRATTA DATI DI NATURA PARTICOLARE INERENTI AI SOGGETTI CON DISABILITA' A FAVORE DEI QUALI E' STATO ISTITUITO IL G.L.O. DI CUI E' MEMBRO FORMALMENTE DESIGNATO DAL DIRIGENTE SCOLASTICO.

Per tutto il tempo in cui svolgerà le predette mansioni nell'ambito di questo Titolare del trattamento;

In modalità che potrà essere sia cartacea che digitale;

Adottando, scrupolosamente, le misure di sicurezza espressamente riportate nel fascicolo allegato recante "Istruzioni Operative", oggetto di formazione specifica che, se non ancora somministrata, lo sarà quanto prima.

Il presente documento non produce effetti giuridici ulteriori rispetto a quelli derivanti dalle Sue mansioni e non è assoggettato ad alcun termine di scadenza, si intende valido fino al passaggio ad altro incarico o cessazione del rapporto intercorrente con il Titolare.

Luogo e data _____

AUTORIZZATO AL TRATTAMENTO (presa visione)

_____

TITOLARE DEL TRATTAMENTO

MICHELE

MICHELE TAMUNNO
23.10.2026
16:11:33
GMT+02:00

_____

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI (Art. 29 Regolamento UE 2016/679 - G.D.P.R.)

Titolare del trattamento dei dati:

ISTITUTO COMPRENSIVO "A. MANZONI"

Via Riccardo Lombardi, 12

20027 RESCALDINA (MI)

Autorizzato al trattamento dei dati:

COLLABORATORE SCOLASTICO

AUTORIZZAZIONE CUMULATIVA

Al fine di poter svolgere regolarmente i compiti inerenti ai seguenti incarichi a Lei assegnati:

A	**Collaboratore scolastico**

appurato che detta attività comporta il trattamento di dati personali e considerato che Lei è in possesso di requisiti di esperienza e capacità tali da fornire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento dei dati, La informo che è autorizzata a trattare i seguenti dati:

	BASE DATI E LORO TIPOLOGIA	CATEGORIE DI INTERESSATI E FINALITA'
A	DATI INERENTI AGLI ALLIEVI [COMUNI] DATI INERENTI AL PERSONALE [COMUNI]	IL COLLABORATORE SCOLASTICO, NELL'AMBITO DELLE PROPRIE MANSIONI DI ACCOGLIENZA E SORVEGLIANZA DEGLI ALLIEVI E DI LORO VIGILANZA ED ASSISTENZA NEI MODI E NEI TEMPI PREVISTI DAL CONTRATTO COLLETTIVO DI RIFERIMENTO, PUO' ACCEDERE AI LORO DATI IDENTIFICATIVI. ACCEDE AI DATI IDENTIFICATIVI DEL PERSONALE SCOLASTICO PER FINALITA' ORGANIZZATIVE IN AFFIANCAMENTO ALLA SEGRETERIA.

Per tutto il tempo in cui svolgerà le predette mansioni nell'ambito di questo Titolare del trattamento;

In modalità che potrà essere sia cartacea che digitale;

Adottando, scrupolosamente, le misure di sicurezza espressamente riportate nel fascicolo allegato recante "Istruzioni Operative", oggetto di formazione specifica che, se non ancora somministrata, lo sarà quanto prima.

Il presente documento non produce effetti giuridici ulteriori rispetto a quelli derivanti dalle Sue mansioni e non è assoggettato ad alcun termine di scadenza, si intende valido fino al passaggio ad altro incarico o cessazione del rapporto intercorrente con il Titolare.

Luogo e data _____

TITOLARE DEL TRATTAMENTO

MICHELE RAMUNNO
23.10.2026 16:11:34 GMT+02:00

AUTORIZZATO AL TRATTAMENTO (presa visione)

MICHELE

_____

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI (Art. 29 Regolamento UE 2016/679 - G.D.P.R.)

Titolare del trattamento dei dati:

ISTITUTO COMPRENSIVO "A. MANZONI"

Via Riccardo Lombardi, 12

20027 RESCALDINA (MI)

Autorizzato al trattamento dei dati:

COMMISSIONE FORMAZIONE CLASSI

AUTORIZZAZIONE CUMULATIVA

Al fine di poter svolgere regolarmente i compiti inerenti ai seguenti incarichi a Lei assegnati:

A	**Membro della commissione di formazione delle classi**

appurato che detta attività comporta il trattamento di dati personali e considerato che Lei è in possesso di requisiti di esperienza e capacità tali da fornire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento dei dati, La informo che è autorizzata a trattare i seguenti dati:

	BASE DATI E LORO TIPOLOGIA	CATEGORIE DI INTERESSATI E FINALITA'
A	DATI INERENTI AGLI ALLIEVI [COMUNI E PARTICOLARI]	ALLIEVI ISCRITTI AL PRIMO ANNO DEL CICLO DI STUDI PER I QUALI SIA NECESSARIO AVERE UN INQUADRAMENTO GENERALE IN ORDINE AL LORO ANDAMENTO SCOLASTICO ED AI LORO BISOGNI EDUCATIVI SPECIFICI AL FINE DI COSTITUIRE GRUPPI CLASSE UNIFORMI

Per tutto il tempo in cui svolgerà le predette mansioni nell'ambito di questo Titolare del trattamento;

In modalità che potrà essere sia cartacea che digitale;

Adottando, scrupolosamente, le misure di sicurezza espressamente riportate nel fascicolo allegato recante "Istruzioni Operative", oggetto di formazione specifica che, se non ancora somministrata, lo sarà quanto prima.

Il presente documento non produce effetti giuridici ulteriori rispetto a quelli derivanti dalle Sue mansioni e non è assoggettato ad alcun termine di scadenza, si intende valido fino al passaggio ad altro incarico o cessazione del rapporto intercorrente con il Titolare.

Luogo e data _____

TITOLARE DEL TRATTAMENTO

MICHELE PAMUNNO 23.10.2026 06:11:34 GMT+02:00

AUTORIZZATO AL TRATTAMENTO (presa visione)

_____

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI (Art. 29 Regolamento UE 2016/679 - G.D.P.R.)

Titolare del trattamento dei dati:

ISTITUTO COMPRENSIVO "A. MANZONI"

Via Riccardo Lombardi, 12

20027 RESCALDINA (MI)

Autorizzato al trattamento dei dati:

COMITATO DI VALUTAZIONE

AUTORIZZAZIONE CUMULATIVA

Al fine di poter svolgere regolarmente i compiti inerenti ai seguenti incarichi a Lei assegnati:

A	**Membro del Comitato di valutazione**

appurato che detta attività comporta il trattamento di dati personali e considerato che Lei è in possesso di requisiti di esperienza e capacità tali da fornire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento dei dati, La informo che è autorizzata a trattare i seguenti dati:

	BASE DATI E LORO TIPOLOGIA	CATEGORIE DI INTERESSATI E FINALITA'
A	DATI IDENTIFICATIVI E DI SERVIZIO INERENTI AL PERSONALE DOCENTE NEOASSUNTO O IN PASSAGGIO DI RUOLO [COMUNI]	DOCENTI NEOASSUNTI O IN PASSAGGIO DI RUOLO PER I QUALI SIA NECESSARIO RICONOSCERE L'ADEGUATEZZA DELLE COMPETENZE PROFESSIONALI IN SEGUITO AD UNA VALUTAZIONE DELLE ATTIVITA' FORMATIVE PREDISPOSTE, DELLE ESPERIENZE DI INSEGNAMENTO E PARTECIPAZIONE ALLA VITA DELLA SCUOLA

Per tutto il tempo in cui svolgerà le predette mansioni nell'ambito di questo Titolare del trattamento;

In modalità che potrà essere sia cartacea che digitale;

Adottando, scrupolosamente, le misure di sicurezza espressamente riportate nel fascicolo allegato recante "Istruzioni Operative", oggetto di formazione specifica che, se non ancora somministrata, lo sarà quanto prima.

Il presente documento non produce effetti giuridici ulteriori rispetto a quelli derivanti dalle Sue mansioni e non è assoggettato ad alcun termine di scadenza, si intende valido fino al passaggio ad altro incarico o cessazione del rapporto intercorrente con il Titolare.

Luogo e data _____

TITOLARE DEL TRATTAMENTO

MICHEL MICHELE PATTUNNO 23.10.2026 16:11:35 GMT+02:00

AUTORIZZATO AL TRATTAMENTO (presa visione)

_____

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI (Art. 29 Regolamento UE 2016/679 - G.D.P.R.)

Titolare del trattamento dei dati:

ISTITUTO COMPRENSIVO "A. MANZONI"

Via Riccardo Lombardi, 12

20027 RESCALDINA (MI)

Autorizzato al trattamento dei dati:

ADDETTO SOMMINISTRAZIONE FARMACI

AUTORIZZAZIONE CUMULATIVA

Al fine di poter svolgere regolarmente i compiti inerenti ai seguenti incarichi a Lei assegnati:

A	**Addetto alla somministrazione di farmaci in orario scolastico**

appurato che detta attività comporta il trattamento di dati personali e considerato che Lei è in possesso di requisiti di esperienza e capacità tali da fornire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento dei dati, La informo che è autorizzata a trattare i seguenti dati:

	BASE DATI E LORO TIPOLOGIA	CATEGORIE DI INTERESSATI E FINALITA'
A	DATI INERENTI AGLI ALLIEVI [COMUNI E PARTICOLARI]	L'ADDETTO CHE HA MANIFESTATO, SU BASE VOLONTARIA, LA PROPRIA DISPONIBILITA', ACCEDE A DATI DI NATURA IDENTIFICATIVA E PARTICOLARE (SALUTE), NEL CASO DI ALLIEVI CHE ABBIANO FATTO RICHIESTA DIRETTAMENTE O MEDIANTE I LORO GENITORI/TUTORI, DI SOMMINISTRAZIONE DI FARMACI IN ORARIO SCOLASTICO.

Per tutto il tempo in cui svolgerà le predette mansioni nell'ambito di questo Titolare del trattamento;

In modalità che potrà essere sia cartacea che digitale;

Adottando, scrupolosamente, le misure di sicurezza espressamente riportate nel fascicolo allegato recante "Istruzioni Operative", oggetto di formazione specifica che, se non ancora somministrata, lo sarà quanto prima.

Il presente documento non produce effetti giuridici ulteriori rispetto a quelli derivanti dalle Sue mansioni e non è assoggettato ad alcun termine di scadenza, si intende valido fino al passaggio ad altro incarico o cessazione del rapporto intercorrente con il Titolare.

Luogo e data _____

TITOLARE DEL T[illegible]

MICHELE R[illegible]

MICHELE RAMUNNO
23.10.2026
16:11:35
GMT+02:00

AUTORIZZATO AL TRATTAMENTO (presa visione)

_____

Istituto Comprensivo " A. MANZONI " - C.F. 84004990150 C.M. MIIC849008 - ABE9D46 - I.C. A. MANZONI RESCALDINA
Prot. 0004604/U del 02/11/2026 I.4 - Archivio, accesso, privacy, trasparenza e relazioni con il pubblico

I ISTRUZIONI
O OPERATIVE
P PRIVACY

REDATTO AI SENSI E PER GLI EFFETTI DELL'ART. 29 REL REGOLAMENTO U.E. 2016/679 AL FINE DI ISTRUIRE GLI AUTORIZZATI AL TRATTAMENTO CIRCA LE MODALITA' DELLO STESSO.

COMPLETO DI:

ISTRUZIONI SPECIFICHE PER L'UTILIZZO RESPONSABILE DELL'INTELLIGENZA ARTIFICIALE

MODELLO REV. 1-2026

CORBELLINI
STUDIO AG.I.COM. Srl

Redatto in collaborazione con:
Studio AG.I.COM. S.r.l. unipersonale del dott. Corbellini
Sede legale: Via XXV Aprile, 12 - 20070 SAN ZENONE AL LAMBRO (MI)
Sede operativa: Viale Campania, 12 – 26855 LODI VECCHIO (LO)
Campus: Via Villa Mari, snc – 06035 GUALDO CATTANEO (PG)
P.IVA, C.F. e C.C.I.A.A. 05078440962 - Capitale sociale: 50.000,00 Euro i.v.

www.agicomstudio.it

SCOPO DEL PRESENTE MANUALE

È da precisare in premessa che le presenti Istruzioni Operative Privacy (I.O.P.), costituiscono parte integrante della lettera di autorizzazione che ha ricevuto in qualità di soggetto che opera all'interno dell'Istituto Scolastico e disciplinano l'uso quotidiano di dati, documenti, account, dispositivi, reti, servizi cloud, applicazioni didattiche e sistemi di intelligenza artificiale in uso e coerenti con le mansioni previste dal suo profilo professionale.

Le regole riportate nel manuale si applicano al personale di segreteria, agli assistenti tecnici, al personale docente, ai supplenti, ai tirocinanti e ai collaboratori che a vario titolo utilizzino sistemi o trattino dati per conto dell'Istituto.

Con la locuzione "istruzioni operative" intendiamo una raccolta di obblighi, indicazioni, procedure e divieti, presentata al fine di ottemperare all'obbligo di cui all'Art. 29 del Regolamento U.E. 2016/679: "*Il responsabile del trattamento o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali, non può trattare tali dati se non è stato istruito in tal senso dal titolare del trattamento...*".

Questo manuale viene messo nella disponibilità di tutti gli autorizzati ed inoltre viene utilizzato come testo di riferimento in occasione dei corsi di formazione che devono essere svolti all'interno dell'Istituto.

Ma qual è lo scopo ultimo che si prefigge l'Istituto fornendo queste istruzioni operative?
Semplificando, ma non troppo, possiamo dire che tutte le istruzioni contenute in questo documento si prefiggono l'obiettivo di scongiurare che dati personali appartenenti ad allievi, dipendenti o fornitori dell'Istituto, vengano divulgati e quindi posti nella disponibilità di chi non è autorizzato a conoscerli (in altre parole l'obiettivo di tutelare la loro privacy).

RIFERIMENTI NORMATIVI ED ORGANIZZATIVI INTERNI

- Regolamento (UE) 2016/679, in particolare artt. 5, 24, 25, 29, 32, 33 e 35;
- D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018;
- Regolamento (UE) 2024/1689 sull'intelligenza artificiale, in particolare art. 4;
- Codice dell'amministrazione digitale e regole organizzative interne;
- Disciplina sul lavoro e sui controlli a distanza;
- Provvedimenti e indicazioni del Garante per la protezione dei dati personali.

Il principio che deve guidare ogni autorizzato al trattamento di dati personali è quello di accedere, usare, comunicare e conservare (ossia "trattare") solo i dati strettamente necessari per il compito assegnato (principio di minimizzazione).
Quando non è chiaro se un'operazione sia consentita, fermarsi immediatamente e chiedere chiarimenti al Dirigente, al DSGA, al referente ICT o al DPO secondo la procedura interna.

DEFINIZIONI

Perché tutti possano comprendere al meglio quanto scritto nel presente manuale, prendendo spunto dall'articolo 4 del Regolamento UE 2016/679 (GDPR), diamo alcune definizioni di base:

Dato anonimo / personale: Si parla di "dato personale" quando ci troviamo di fronte ad una informazione riferibile ad una persona fisica identificabile (ad es. Mario Rossi di 3C ha i capelli biondi), mentre se l'informazione non fa riferimento a nessuno nello specifico (p.es. il 30% degli allievi che frequentano l'Istituto ha i capelli biondi) allora siamo di fronte ad un dato anonimo.
Le normative sulla privacy, dalla loro nascita a tutt'oggi, tutelano solo ed esclusivamente i dati personali.
E' chiaro a tutti che il livello di tutela richiesto dipende non solo dal fatto che il dato sia personale, ma anche dalla delicatezza dell'informazione.
Una informazione come "*essere portatore di disabilità*" è ovviamente molto più delicata rispetto ad "*avere i capelli biondi*" e quindi la normativa ha introdotto, potremmo dire, diverse gradazioni del concetto di dato personale: il dato comune, il dato particolare ed il dato giudiziario.

Dato comune / particolare / giudiziario: Un dato personale si dice "particolare" quando fa riferimento: allo stato di salute, all'orientamento sessuale, all'orientamento politico o alla fede religiosa di un soggetto. Si parla inoltre di dato particolare quando si tratta di informazioni genetiche (D.N.A. etc.) o biometriche (impronte digitali etc.).

Con il termine "dato giudiziario" invece si intendono i precedenti penali ed i carichi pendenti di un soggetto, ossia i suoi trascorsi giudiziari. Tutti i dati che, pur essendo personali, non rientrano nelle definizioni sopra date (anagrafici, andamento scolastico, importo dello stipendio, orari etc.) si definiscono "dati comuni".
È bene precisare che, anche i dati comuni, in quanto dati personali, sono tutelati ma con una intensità minore rispetto a quanto non sia previsto per i dati particolari e giudiziari.

Trattamento: senza scomodare la definizione di legge, possiamo ben dire che costituisce un trattamento di dato personale qualsiasi operazione io svolga con un dato personale (raccolta, registrazione, organizzazione, trasmissione, cancellazione etc.) anche la mera detenzione.
Questo significa che la sola custodia all'interno della nostra borsa di un foglietto riportante il numero di telefono di un allievo o la memorizzazione del medesimo numero sul nostro telefono, costituisce un trattamento di dato personale ed è quindi regolamentato dalla legge.
Nel primo caso (foglietto in borsa) saremo di fronte ad un trattamento di dato in formato cartaceo, nel secondo caso (memorizzazione nel telefono) in formato digitale.

Titolare del Trattamento: È l'Istituto Scolastico, incarnato nella persona che ne ha la rappresentanza legale. Nel caso delle Scuole Statali, tale incarico è del Dirigente Scolastico, mentre per le Scuole Paritarie, dipende dalla loro forma giuridica (società, cooperativa, ente etc.).

Autorizzato al Trattamento: Partendo dal presupposto che il Titolare del Trattamento, da solo, non può portare avanti l'intera attività scolastica, tutti i suoi collaboratori interni che lo affiancano nell'attività (Segreteria, Docenti, Collaboratori Scolastici, Assistenti Tecnici etc.) sono da considerarsi "Autorizzati al Trattamento".
Naturalmente non tutte le autorizzazioni hanno lo stesso perimetro, esistono autorizzazioni molto ampie (Collaboratore vicario, D.S.G.A., Segretario Generale etc.), altre più ridotte (Docente che presta servizio in 2B, Assistente Amministrativo etc.) ed altre ancora solo eventuali (Collaboratore Scolastico, Ausiliario, Tecnico etc.).
Il perimetro dell'autorizzazione è evidenziato nella lettera di autorizzazione a cui il presente manuale è allegato.

Responsabile del Trattamento: Il concetto è affine a quello sopra definito di autorizzato, cambia il fatto che il responsabile è normalmente un soggetto esterno (che quindi non ha un contratto di lavoro con la scuola), con una propria organizzazione autonoma, a cui l'Istituto attribuisce compiti di trattamento dati (gestore del registro elettronico, della segreteria digitale, tesoreria, RSPP, DPO, etc.).
In questo caso la sua designazione avviene mediante un vero e proprio contratto.

ISTRUZIONI COMUNI A TUTTO IL PERSONALE

Elenchiamo alcune regole generali valide per tutti gli operatori scolastici:

PRINCIPI GENERALI	Rispettare i principi generali del GDPR, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi. **È vietato trattare i dati in modo diverso rispetto a quanto previsto dalle procedure interne**, inoltre i dati possono essere usati esclusivamente per finalità compatibili con l'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti scolastici. È vietato sia modificare le modalità di svolgimento dei trattamenti esistenti che introdurre nuovi trattamenti senza l'esplicita autorizzazione del titolare del trattamento;
RISERVATEZZA DEI DATI	Rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto; **Non consultare fascicoli, registri, archivi o profili per curiosità** o per favorire terzi.
	Non discutere casi individuali in corridoi, sale comuni, chat informali o davanti a persone non autorizzate;
INTEGRITA' DEI DATI	Rispettare le misure di sicurezza digitali, comportamentali e organizzative prescritte, atte a salvaguardare la riservatezza e l'integrità dei dati;
DATA BREACH E MIGLIORIE	Segnalare senza ritardo al proprio superiore gli eventuali malfunzionamenti degli strumenti elettronici e le eventuali perdite di dati. Segnalare anche tutte le esigenze organizzative e tecniche, che possono migliorare lo svolgimento delle operazioni affidate; Le problematiche che impattano sui dati personali possono costituire un *data breach* per il quale sussiste l'obbligo di notifica entro 72 ore al Garante, di conseguenza è fondamentale

	informare senza ritardo il proprio responsabile in caso di incidente di sicurezza che coinvolga dati particolari e no. **Segnalare immediatamente errori di invio, smarrimenti, accessi sospetti, malware e ogni possibile violazione.** Non cancellare evidenze di un incidente e non tentare riparazioni autonome che possano aggravarlo;
INTERRUZIONE DEL LAVORO	Se fosse necessario interrompere il lavoro, anche temporaneamente, verificare che i dati trattati non siano accessibili a terzi non autorizzati (ad esempio tramite PC lasciati accesi o armadi e schedari lasciati aperti). **Bloccare sempre lo schermo quando ci si allontana e fare logout dai servizi condivisi;**
CREDENZIALI DI ACCESSO	Mantenere strettamente riservate le proprie credenziali di autenticazione;
MINIMIZZAZIONE	Ridurre al minimo dati, destinatari, copie, allegati, stampe e tempi di conservazione;
IDENTIFICAZIONE DEI RICHIEDENTI	Verificare identità e legittimazione di chi richiede informazioni, soprattutto al telefono o via e-mail.
PIATTAFORME AUTORIZZATE	Utilizzare solo account, piattaforme, APP e dispositivi autorizzati dall'Istituto.
DATI PARTICOLARI E GIUDIZIARI	**Rispettare le istruzioni più restrittive previste per dati sanitari, disabilità, situazioni familiari, dati giudiziari e altri dati particolari.**

ISTRUZIONI DIFFERENZIATE PER RUOLO

A seguire elenchiamo le regole specificamente pensate per i singoli ruoli scolastici:

RUOLO	COSA PUO' FARE	COSA DEVE EVITARE
PERSONALE ADDETTO ALLA SEGRETERIA	• Gestire fascicoli, protocollo, personale, allievi, contabilità e comunicazioni nei limiti dell'area assegnata; • Comunicare usando i canali istituzionali; • Verificare con scrupolo destinatari delle comunicazioni e allegati.	• Esportazioni massive non necessarie; • Invii in chiaro di dati delicati; • Uso di cloud o e-mail personali; • Consultazione di pratiche estranee.
PERSONALE TECNICO	• Amministrare i sistemi e le piattaforme secondo incarico ricevuto; • Applicare gli aggiornamenti; • Verificare il funzionamento di backup, e la corretta implementazione delle autorizzazioni e delle misure di sicurezza.	• Accedere al contenuto dei dati oltre quanto indispensabile; • Usare account condivisi senza tracciabilità; Copiare dati su propri supporti; • Modificare i log.
DOCENTI	• Usare esclusivamente il registro elettronico e le piattaforme didattiche ed i sistemi di I.A. autorizzati; • Trattare solo i dati degli alunni delle classi assegnate; • Comunicare tramite canali ufficiali.	• Pubblicare voti, diagnosi o situazioni personali nelle chat; • Usare account personali; • Creare gruppi non autorizzati; • Caricare elaborati identificabili in servizi I.A. non approvati.

ISTRUZIONI OPERATIVE SPECIFICHE PER SCENARI DIVERSI

A seguire elenchiamo le regole specificamente pensate per specifici scenari presenti a scuola:

DOCUMENTI CARTACEI, LOCALI E ATTIVITA' DI SPORTELLO	Applicare la regola della **scrivania pulita**: documenti e registri non devono restare esposti quando la postazione non è presidiata.
	Custodire fascicoli e supporti in **armadi o cassetti chiusi;** le chiavi sono affidate solo al personale autorizzato.
	Regolare l'accesso a segreteria, direzione, CED e archivi; i visitatori non devono rimanere soli.
	Consegnare documenti solo dopo **verifica dell'identità**, della delega e dell'effettivo diritto a riceverli.
	Usare buste o cartelline coprenti per trasferire documenti delicati.
	Ritirare subito le stampe e controllare che fotocopiatrici e scanner non conservino documenti o file accessibili.
	Distruggere gli scarti con distruggidocumenti; non gettare fogli leggibili nei cestini.
	Allo sportello e al telefono **usare tono di voce contenuto** e non pronunciare informazioni eccedenti.
ACCOUNT & PASSWORD	Ogni **utenza deve essere nominale.** **È vietato usare l'account di un collega** o lasciare sessioni aperte per altri.
	Usare **password complesse** (almeno 8 caratteri, composte da maiuscole, minuscole, numeri e caratteri speciali), non riconducibili alla persona; preferire *passphrase* (sequenza di parole o frasi più lunghe rispetto a una password tradizionale). Non riutilizzarla al suo cambio.
	Attivare **l'autenticazione a più fattori** quando disponibile e non approvare richieste MFA inattese.
	Non comunicare password, codici OTP o codici di recupero, neppure a chi dichiara di essere assistenza tecnica.
	Cambiare subito la password quando si sospetta compromissione, dopo comunicazione accidentale o su richiesta motivata del servizio tecnico; seguire l'eventuale policy di rotazione dell'Istituto.
	Non conservare password su fogli visibili, file non protetti o browser personali. Usare solo il gestore di credenziali autorizzato, se presente.
	Gli account privilegiati degli amministratori devono essere separati dagli account ordinari e usati solo per attività amministrative.

Una richiesta urgente di password, OTP, bonifico, modifica IBAN o apertura di un file deve essere verificata con un secondo canale conosciuto, mai usando i recapiti contenuti nel messaggio sospetto.

POSTA ELETTRONICA P.E.C. MESSAGGISTICA	**Usare la casella istituzionale per le attività di servizio.** Le comunicazioni ufficiali seguono le regole di protocollo e firma dell'Istituto.
	Prima dell'invio **verificare destinatari**, campo A/CC/CCN, oggetto, allegati e presenza di dati non necessari.
	Usare CCN per comunicazioni collettive quando i destinatari non devono conoscere gli indirizzi altrui.
(segue)	**Per dati particolari o giudiziari usare il canale istituzionale più sicuro** disponibile; se si invia un file cifrato, comunicare la password con canale separato.
	Non inoltrare documenti scolastici a e-mail personali e non sincronizzare la posta su dispositivi non autorizzati.
	Diffidare di mittenti insoliti, domini simili ma non identici, urgenze, errori linguistici, QR code, link abbreviati e allegati inattesi.
POSTA ELETTRONICA P.E.C. MESSAGGISTICA	**Non aprire macro o file eseguibili.** In caso di dubbio contattare il mittente tramite recapito noto e segnalare al referente ICT.
	Le chat non sostituiscono registro elettronico, protocollo o posta istituzionale. Non pubblicare in chat voti, certificazioni, diagnosi o immagini non necessarie.

DISPOSITIVI RETE CLOUD SUPPORTI REMOVIBILI	**Usare dispositivi gestiti e aggiornati dall'Istituto.** Non disattivare antivirus, firewall, cifratura o altri controlli.
	Installare software, estensioni e app solo tramite il servizio tecnico o con sua autorizzazione.
	Salvare i documenti nelle aree istituzionali previste, non sul desktop locale se non temporaneamente e non su cloud personali.
	Non collegare chiavette o dischi personali. I supporti autorizzati vanno cifrati, custoditi e sottoposti a scansione.
	Non usare reti Wi-Fi pubbliche per trattamenti delicati senza le protezioni disposte dall'Istituto; evitare hotspot personali per aggirare filtri e controlli.
	Custodire notebook e tablet durante gli spostamenti; non lasciarli visibili in auto e segnalare immediatamente furto o smarrimento.
	Prima della riassegnazione o dismissione, affidare il dispositivo al servizio tecnico per cancellazione sicura e tracciata.
	Non fotografare schermi, registri o documenti con smartphone personali.
IGIENE INFORMATICA CYBERSECURITY	ROUTINE QUOTIDIANA:
	Riavviare il dispositivo quando richiesto per completare gli aggiornamenti.
	Bloccare lo schermo anche per assenze brevi.
	Chiudere applicazioni e schede non necessarie.
	Controllare l'indirizzo reale dei link prima di aprirli.
	Segnalare rallentamenti anomali, finestre insolite, richieste MFA inattese o accessi da luoghi sconosciuti.
	A fine attività chiudere le sessioni, ritirare le stampe e riporre i supporti.
	IN CASO DI SOSPETTA COMPROMISSIONE:
	Interrompere l'operazione e non inserire altre credenziali.
	Se ragionevolmente possibile, disconnettere il dispositivo dalla rete senza cancellare file o spegnerlo, salvo diversa istruzione del servizio tecnico.
	Avvisare immediatamente il referente ICT e il responsabile interno privacy, indicando ora, dispositivo, account e operazione svolta.
	Conservare il messaggio, l'allegato, l'indirizzo del sito e una schermata dell'errore.
	Cambiare le credenziali da un dispositivo sicuro solo seguendo le indicazioni ricevute.

ISTRUZIONI OPERATIVE SPECIFICHE PER IL PERSONALE DOCENTE

REGISTRO ELETTRONICO DIDATTICA DIGITALE SOCIAL IMMAGINI	**Il registro elettronico è personale**: non lasciare la sessione aperta e non consentire l'uso delle proprie credenziali ad alunni o colleghi.
	Inserire annotazioni pertinenti e professionali, evitando dettagli sanitari o familiari non necessari.
	Usare solo classi virtuali e repository autorizzati. Configurare correttamente condivisioni, gruppi e scadenze dei link.
	Non pubblicare foto, video, audio, lavori o dati degli alunni su profili personali. I canali istituzionali seguono informative, basi giuridiche e procedure approvate.
	Non creare gruppi di messaggistica con studenti o famiglie fuori dalle regole dell'Istituto. Le chat non sono luogo per valutazioni o casi personali.
	Durante videolezioni o riunioni verificare partecipanti, sfondo, condivisione schermo e documenti visibili; non registrare senza specifica autorizzazione e informazione.

ISTRUZIONI OPERATIVE SPECIFICHE PER IL PERSONALE TECNICO

PIATTAFORME DI ISTITUTO	**Applicare il principio del minimo privilegio** (policies) e rivedere periodicamente account, gruppi, permessi e utenze non più necessarie.
	Usare account amministrativi nominativi, MFA e registrazione degli accessi; evitare credenziali condivise.
	Pianificare aggiornamenti, backup e prove di ripristino; documentare esiti e anomalie.
	Proteggere console, apparati di rete, telecamere e sistemi remoti con segmentazione, cifratura e accessi limitati.
	Accedere ai contenuti degli utenti solo se indispensabile per l'intervento, secondo incarico e procedura; evitare copie non necessarie.
	Concordare l'assistenza remota, renderla visibile all'utente quando possibile e chiudere la sessione al termine.
	Conservare i log per il periodo definito dall'Istituto e impedirne alterazione o accesso non autorizzato.
	Gestire fornitori, manutentori e responsabili esterni assicurando autorizzazioni, tracciabilità e restituzione/cancellazione dei dati.
	In caso di vulnerabilità critica, isolare il rischio e attivare la procedura di incidente senza occultare o minimizzare l'evento.

ISTRUZIONI OPERATIVE SPECIFICHE PER LA VIDEOSORVEGLIANZA

VIDEOSORVEGLIANZA	Solo i soggetti formalmente autorizzati possono accedere al locale, al sistema o alle immagini.
	Le credenziali sono individuali; ogni consultazione, estrazione o consegna deve essere motivata e tracciata.
	È vietato usare le immagini per curiosità, controllo informale del personale o finalità diverse da quelle dichiarate.
	Le immagini sono conservate per il periodo definito nella policy e cancellate automaticamente, salvo specifica esigenza documentata o richiesta dell'autorità.
	Non fotografare monitor o condividere filmati tramite app o dispositivi personali.
	Le richieste di accesso o acquisizione sono inoltrate al referente individuato dall'Istituto; il personale non consegna copie di propria iniziativa.
	Guasti, accessi sospetti e variazioni dell'inquadratura devono essere immediatamente segnalati.

ISTRUZIONI OPERATIVE SPECIFICHE PER L'UTILIZZO RESPONSABILE DELL'INTELLIGENZA ARTIFICIALE

I sistemi di IA possono supportare attività redazionali, organizzative e didattiche, ma non sostituiscono la responsabilità professionale, il controllo umano e le procedure dell'Istituto.
L'uso degli stessi è consentito limitatamente a quanto previsto dallo specifico regolamento di istituto e solo per gli strumenti e le finalità autorizzate (white list).

	REGOLA
SISTEMI DI INTELLIGENZA ARTIFICIALE	Non inserire in sistemi IA nomi, cognomi, e-mail, immagini, voci, elaborati identificabili, diagnosi, PEI/PDP, dati disciplinari, giudiziari, economici e dati personali in genere. Tale divieto è da intendersi assoluto se l'utilizzo del sistema è ancora in fase sperimentale e se non è stato espressamente autorizzato dal titolare del trattamento.
	Prima di usare un servizio IA verificare che sia incluso nell'elenco degli strumenti approvati (white list) e seguire le impostazioni del regolamento.
	Preferire dati anonimi o sintetici. Rimuovere identificativi diretti e indiretti; la sola sostituzione del nome spesso non rende anonimo un caso.
	Non usare l'IA per assumere autonomamente decisioni che producono effetti su studenti o personale, inclusi voti, ammissioni, sanzioni, selezioni, profili di rischio o diagnosi.
	Controllare sempre accuratezza, completezza, fonti, tono, possibili pregiudizi e rispetto del diritto d'autore. L'output può contenere errori o informazioni inventate.
	Dichiarare l'uso dell'IA quando previsto dalle regole dell'Istituto o quando incide in modo significativo sul contenuto prodotto (trasparenza).
	Non generare o diffondere immagini, audio o video realistici di persone senza base giuridica, autorizzazione e chiara finalità istituzionale.
	Non chiedere all'IA di imitare persone reali, ricostruire dati mancanti o dedurre salute, fragilità, convinzioni, comportamento o rendimento individuale.
	Conservare solo gli output necessari, nelle aree istituzionali, applicando limiti di accesso e tempi di conservazione.
	Partecipare alle attività di alfabetizzazione IA organizzate dall'Istituto e segnalare usi impropri o risultati potenzialmente dannosi.

ESEMPI DI UTILIZZO DELL'I.A. AMMESSI E NO, PER RUOLO

RUOLO	USO PRUDENTE	USO VIETATO / DA AUTORIZZARE
PERSONALE ADDETTO ALLA SEGRETERIA	• bozza di testo generico senza dati reali, poi verificata dal personale.	• caricare un fascicolo, un ricorso, un contratto o un elenco nominativo in un chatbot non autorizzato.
PERSONALE TECNICO	• supporto su configurazioni con log anonimizzati e senza dati segreti.	• incollare credenziali, chiavi API, configurazioni complete, log con utenti o vulnerabilità in servizi esterni.
DOCENTI	• creare esercizi generici e rubriche, con revisione professionale.	• far correggere elaborati identificabili o generare automaticamente voti e giudizi individuali.

VIOLAZIONI DI DATI PERSONALI E INCIDENTI – IL DATA BREACH

Viene definita come *data breach* qualsiasi perdita, distruzione, modifica, divulgazione o accesso non autorizzato a dati personali, anche accidentale.

Esempi: e-mail inviata al destinatario sbagliato, allegato errato, registro smarrito, account compromesso, malware, chiavetta persa, documento pubblicato online, condivisione cloud aperta, fascicolo consultato da persona non autorizzata.

	PROCEDURA
DATA BREACH	**Segnalare senza ritardo l'evento che si suppone costituire un data breach** al Dirigente/DSGA o referente designato e al canale interno previsto, anche se l'errore sembra lieve.
	Indicare cosa è accaduto, quando è stato scoperto, dati e persone coinvolte, destinatari, sistemi interessati e prime misure adottate.
	Non contattare autonomamente gli interessati o il Garante, salvo che ciò non costituisca un'istruzione del Titolare.
	Non cancellare nulla (messaggi, log o file utili alla ricostruzione).
	Collaborare alle misure di contenimento. Sarà il Titolare, con DPO e tecnici, a valutare rischio, documentazione, eventuale notifica e comunicazione.

Tempo critico:
La normativa prevede, quando ne ricorrono i presupposti, la notifica del Titolare all'autorità di controllo (Garante Privacy) entro 72 ore dal momento in cui ne è venuto a conoscenza.
Per questo la segnalazione interna deve essere immediata.

DIECI REGOLE DI BUONSENSO

Pensa prima di cliccare.
Controlla due volte prima di inviare.
Se non serve, non raccoglierlo e non conservarlo.
Se non sei autorizzato, non aprirlo.
Se è delicato, usa il canale più sicuro.
Se ti allontani, blocca lo schermo.
Se un messaggio crea urgenza o paura, verifica con un secondo canale.
Se uno strumento è gratuito ma non approvato, non usarlo con dati scolastici.
Se l'IA produce un testo, resta tua la responsabilità di verificarlo.
Se hai commesso un errore, segnalalo subito: nasconderlo aumenta il rischio.

FONTI E DOCUMENTI DI RIFERIMENTO

- Regolamento (UE) 2016/679 (GDPR).
- D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018.
- Regolamento (UE) 2024/1689 (AI Act), con particolare riferimento all'art. 4 sull'alfabetizzazione in materia di IA.
- Garante per la protezione dei dati personali, materiali tematici "Scuola" e "Intelligenza artificiale", incluso il vademecum "La scuola a prova di privacy".
- Documenti interni Studio AG.I.COM.: IOP - Istruzioni Operative; MdP - Manuale delle Procedure Privacy; Manuale Privacy Videosorveglianza; Regolamento Internet e Mail; Regolamento Videosorveglianza; Regolamento Privacy Segreteria; Regolamento uso social.

MICHELE
RAMUNNO
23.10.2026
16:11:17
GMT+02:00