



## **MODELLO ORGANIZZATIVO DEL LICEO SCIENTIFICO A. ROMITA DI CAMPOBASSO IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI, IN APPLICAZIONE DEL REGOLAMENTO (UE) 2016/679 (GDPR).**

### **Art. 1**

#### **Oggetto e ambito di applicazione**

1. Il Liceo Scientifico Statale A. Romita è il Titolare del trattamento dei dati personali.
2. Il presente modello individua i soggetti mediante i quali il Liceo esercita le funzioni di Titolare del trattamento dei dati personali.
3. Le disposizioni contenute nel presente documento si applicano a tutte le strutture organizzative del Liceo A. Romita

### **Art. 2**

#### **Attribuzioni delle competenze del titolare**

1. Le competenze del Titolare previste nel GDPR sono attribuite al Dirigente Scolastico, cui spettano i seguenti compiti:
  - a. designare e nominare gli organismi monocratici e collegiali previsti dalla normativa e rimessi alla determinazione del titolare con particolare riferimento alla nomina del DPO-RPD;
  - b. verificare la legittimità dei trattamenti di dati personali effettuati all'interno dell'Istituzione Scolastica;
  - c. disporre, in conseguenza alla verifica di cui alla lett. b., le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
  - d. verificare e attuare il costante aggiornamento del Registro delle attività di trattamento previsto dall'art. 30 del GDPR;
  - e. garantire la corretta informazione e l'esercizio dei diritti degli interessati;
  - f. verificare l'aggiornamento della modulistica in coerenza con la normativa sulla Privacy;
  - g. curare la formazione del personale dell'Istituzione Scolastica in materia di trattamento dei dati personali;
  - h. fornire le istruzioni necessarie per il corretto trattamento dei dati personali;
  - i. verificare che i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "autorizzati") operino nel rispetto delle istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni e linee guida generali e specifiche impartite (allegato A – ALL.B) e fornendo ogni altra istruzione che si riterrà necessaria e specifica per i diversi soggetti autorizzati al trattamento;
  - j. individuare i Responsabili esterni del trattamento e perfezionare gli atti previsti dall'art. 28 del GDPR;
  - k. attivare senza indugio, in caso di incidenti che riguardano la sicurezza dei dati (Data Breach) la Struttura di Coordinamento Privacy e collaborare con essa per la gestione dell'incidente;
  - l. effettuare, nei casi previsti dall'art. 35 del GDPR, la Valutazione d'Impatto sulla protezione dei dati;
  - m. consultare il DPO/RPD per ogni questione di interesse afferente l'applicazione del GDPR,
  - n. verificare il costante aggiornamento dell'albo on line, contemperando le esigenze di trasparenza e pubblicità legale con i principi e i limiti imposti dalle norme sul trattamento dei dati personali.



### **Art. 3**

#### **Struttura di Coordinamento Privacy**

1. In assistenza al Titolare è costituito un gruppo di gestione delle attività di trattamento diretto da DSGA, costituito da: DSGA Maria Vittoria Dina Genovese, assistente amministrativo Marina De Castro, assistente tecnico Marina Alfiero.

Al gruppo compete di sovrintendere al coordinamento generale delle funzioni e attività in materia di trattamento dati personali con particolare riferimento:

- a. alla gestione delle relazioni con il DPO/RPD;
- b. all'organizzazione della formazione rivolta al personale dell'Istituto;
- c. all'aggiornamento della modulistica;
- d. all'aggiornamento del Registro delle attività di trattamento;
- e. alla corretta informazione verso gli interessati e all'esercizio dei loro diritti;
- f. alla formulazione di istruzioni in materia di trattamento dati personali e alla verifica della loro applicazione;
- g. alla gestione degli incidenti che riguardano la sicurezza dei dati (Data Breach);
- h. alle Valutazioni d'Impatto sulla protezione dei dati.

### **Art. 4**

#### **Autorizzazione al trattamento**

1. I dipendenti dell'Istituzione Scolastica (Docenti, Assistenti Amministrativi, Collaboratori Scolastici, Assistenti tecnici) e i soggetti che operano ad altro titolo nell'ambito della stessa, sotto l'autorità del titolare, sono autorizzati al trattamento dei dati personali gestiti dall'Istituzione Scolastica in base alle specifiche competenze, al ruolo, alle funzioni ed agli incarichi ricevuti, nel rispetto delle istruzioni generali e specifiche allegate al presente Modello e di ogni altra istruzione che il Titolare riterrà di impartire.



## **Allegato A**

### **ISTRUZIONI AGLI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI**

Il trattamento dei dati da parte degli autorizzati dovrà avvenire nel rispetto dei principi del Regolamento (UE) 2016/679 (GDPR) e delle ulteriori disposizioni impartite.

L'accesso ai dati è consentito per quanto strettamente necessario per adempiere ai compiti individualmente assegnati, con divieto di qualunque diversa utilizzazione, funzione e divulgazione non espressamente autorizzata dal Titolare del trattamento.

Per il trattamento dei dati personali, è necessario attenersi alle seguenti Istruzioni e Linee guida di sicurezza generali:

#### **Istruzioni**

1. Trattare i dati personali in modo lecito e secondo correttezza;
2. Raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in modalità compatibili con tali scopi;
3. Verificare che siano esatti e, se necessario, aggiornarli;
4. Verificare che siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
5. Non comunicare a terzi, al di fuori dell'ambito lavorativo o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
6. Accertarsi dell'identità degli interessati prima di fornire informazioni circa i dati personali o il trattamento effettuato.
7. non comunicare dati personali via telefono o via email se non si ha assoluta certezza dell'identità del destinatario delle comunicazioni;
8. non comunicare e non diffondere qualsiasi dato personale o qualsiasi informazione relativa alla vita, all'attività, alla comunità scolastica se non si è autorizzati o se la stessa comunicazione/diffusione non sia necessaria per le finalità istituzionali della scuola;
9. non usare canali di comunicazione di gruppo o strumenti non autorizzati per diffondere dati personali e informazioni inerenti la vita e la comunità scolastica;
10. segnalare immediatamente, al titolare o al DSGA, ogni eventuale evento che possa configurare o determinare un accesso indebito, una modifica, una perdita di dati personali o comunque ogni altra violazione degli stessi;
11. Accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
12. Accertarsi dell'identità degli interessati e della loro autorizzazione al trattamento e dell'eventuale autorizzazione scritta a terzi, al momento del ritiro di documentazione in uscita.

#### **Linee guida di sicurezza/documenti cartacei**

1. Conservare sempre i dati del cui trattamento si è incaricati in apposito armadio o cassetto assegnato, dotato di serratura;
2. Accertarsi della corretta funzionalità dei meccanismi di chiusura degli armadi e/o dei cassetti, segnalando tempestivamente al proprio responsabile eventuali anomalie o rischi;
3. Non consentire l'accesso alle aree in cui sono conservati dati personali su supporto cartaceo a estranei e a soggetti non autorizzati;
4. Non consentire l'accesso a estranei ai fax, ai fotocopiatori e alle stampanti che contengano documenti non ancora ritirati dal personale;
5. Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;



6. Provvedere personalmente alla distruzione dei dati quando è necessario eliminare documenti inutilizzati, facendo in modo che essi non siano più ricomponibili;
7. Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o particolari, ma accertarsi che vengano sempre distrutte;
8. Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti presenti sulla stessa;
9. Segnalare immediatamente al proprio responsabile la presenza di documenti incustoditi, provvedendo temporaneamente alla loro custodia;
10. 10. Segnalare immediatamente al titolare ogni eventuale perdita, modifica, diffusione indebita di documenti contenenti dati personali di cui si viene a conoscenza.

#### **Linee guida di sicurezza/Dati e supporti informatici**

1. Non lasciare supporti di memorizzazione, cartelle o altri documenti a disposizione di estranei;
2. Conservare i supporti contenenti dati personali in armadi o cassetti chiusi, ad accesso controllato o in file protetti da password;
3. Riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori, armadi, cassetti dove sono custoditi;
4. Non consentire l'accesso ai dati a soggetti non autorizzati;
5. Non riutilizzare i supporti informatici utilizzati per il trattamento di dati particolari per altri trattamenti;
6. Segnalare immediatamente al proprio responsabile la perdita di supporti contenenti dati personali.

#### **Linee guida di sicurezza/Password**

1. Scegliere una password che abbia le seguenti caratteristiche:
  - sia originale;
  - sia composta almeno da otto caratteri;
  - contenga caratteri di almeno 4 diverse tipologie, da scegliere tra: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (cioè punti, trattino, underscore, ecc.);La password non deve contenere riferimenti personali facili da indovinare (nome, cognome, data di nascita, ecc.); non deve nemmeno contenere riferimenti al nome utente (detto anche user account, alias, user id, user name);
2. curare la conservazione della propria password ed evitare di comunicarla ad altri;
3. Non fare digitare la propria password a terzi che stanno operando sui computer o su altri dispositivi di lavoro;
4. Non scrivere mai le proprie password su taccuini, fogli o ogni altro oggetto che possa distrattamente e facilmente perdersi oppure su file non protetti dei propri dispositivi personali eventualmente usati per attività lavorative;
5. Cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
6. Non condividere password via email, sms, social network, instant messaging, ogni altro mezzo di comunicazione telematica;
7. Non comunicare la password a nessuno e non farla digitare a terzi che eventualmente stiano operando sui computer;
8. Non utilizzare password già utilizzate in passato;
9. Sostituire immediatamente password rilasciate da un sistema o un sistema informatico, cambiandole con password che seguano le regole di cui ai punti precedenti.



#### **Linee guida di sicurezza/Postazione di lavoro**

1. Proteggere la propria postazione di lavoro con una password;
2. Spegnerne correttamente il computer o altri dispositivi usati al termine dell'attività;
3. Non lasciare incustodita la propria postazione di lavoro per la pausa o altri motivi senza averla spenta o essersi disconnessi dalle sessioni attive e aver inserito uno screen saver con password;
4. Comunicare tempestivamente al proprio responsabile qualunque anomalia riscontrata nel funzionamento del computer.

#### **Linee guida di sicurezza/Posta elettronica**

1. Non aprire documenti di cui non sia certa la provenienza;
2. Non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
3. Controllare accuratamente l'indirizzo dei destinatari prima di inviare dati personali.

**In caso di attivazione della modalità di lavoro di cui agli artt. 18-24 della Legge 22 maggio 2017 n. 81 (smart working o lavoro agile) o di svolgimento di attività didattiche e formative a distanza, oltre alle suddette, è necessario attenersi alle seguenti, ulteriori istruzioni:**

- Avere un pc con sistema operativo aggiornato;
- Avere un antivirus e verificare che sia aggiornato;
- Creare un account specifico per l'uso nei momenti di lavoro, se il pc è usato anche da familiari o conviventi.

Le medesime istruzioni di sicurezza devono essere seguite anche in caso di svolgimento dell'attività professionale attraverso tablet, smartphone o altri strumenti elettronici.



## **ALL.B - ISTRUZIONI SPECIFICHE**

### **LINEE GUIDA IN MATERIA DI SICUREZZA PER IL DOCENTE INCARICATO DEL TRATTAMENTO**

Il docente deve attenersi scrupolosamente alle suddette e alle seguenti, ulteriori indicazioni per garantire la sicurezza dei dati personali trattati:

Per il trattamento dei dati sui computer e dispositivi presenti nelle aree e nei laboratori (Registro Elettronico, Aula di informatica, Aula Docenti, Laboratori,...) seguire le seguenti istruzioni:

1. Non lasciare supporti di memorizzazione (CD/DVD, Dispositivi USB, ...), cartelle o altri documenti a disposizione di estranei;
2. non consentire l'accesso ai dati a soggetti non autorizzati;
3. riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove essi sono custoditi;
4. non memorizzare o non riportare dati personali (propri e di altre persone) sui computer o su altri strumenti utilizzati per la didattica.

Per i dati cartacei:

1. Tutta la documentazione che contiene dati personali degli alunni deve essere custodita in un apposito armadio a cassetto, dotato di serratura, la cui chiave non deve esser lasciata incustodita;
2. i certificati medici a giustificazione delle assenze per malattia degli alunni, una volta esibiti, dovranno essere consegnati immediatamente all'Ufficio di Segreteria, che ne curerà l'acquisizione al fascicolo personale dell'alunno interessato;
3. le prove personali degli alunni sono custodite nel cassetto personale e poi consegnate all'Ufficio di Segreteria che ne curerà la custodia.
4. Ogni docente è responsabile della corretta tenuta del cassetto, della sua regolare chiusura ed è obbligato a segnalare ogni inconveniente che possa compromettere la custodia o il suo regolare funzionamento.

Altre istruzioni

1. Non comunicare e non diffondere dati e informazioni di natura personale che non siano necessari per lo svolgimento delle attività didattiche;
2. Non comunicare né diffondere informazioni sullo stato di salute o comunque informazioni di natura particolare ex artt.9-10 del GDPR acquisite o comunque di cui si viene a conoscenza, al di fuori degli stretti obblighi di natura professionale;
3. Non realizzare e non diffondere foto, filmati, audio relativi alla vita scolastica e didattica, se non specificamente autorizzati;
4. Non comunicare e non diffondere informazioni riferite a specifici alunni, genitori, personale, a terzi, attraverso canali di comunicazione privata.

### **LINEE GUIDA IN MATERIA DI SICUREZZA PER L'ASSISTENTE AMMINISTRATIVO INCARICATO DEL TRATTAMENTO**

L'assistente amministrativo deve attenersi scrupolosamente alle suddette e alle seguenti indicazioni per garantire la sicurezza dei dati personali trattati:

1. Conservare sempre i dati del cui trattamento si è incaricati in apposito armadio o cassetto assegnato, dotato di serratura;
2. Accertarsi della corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente al proprio Responsabile eventuali anomalie;



3. Non consentire l'accesso alle aree in cui sono conservati dati personali su supporto cartaceo a estranei e a soggetti non autorizzati;
4. Conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti;
5. Consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti;
6. Non consentire l'accesso a estranei al fax, alle fotocopiatrici, alle stampanti contenenti documenti non ancora ritirati dal personale;
7. Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;
8. Provvedere personalmente alla distruzione di documenti inutilizzati che è necessario eliminare;
9. Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengano dati personali o particolari, ma accertarsi che esse vengano sempre distrutte;
10. Non lasciare incustodito il registro contenente gli indirizzi, i recapiti telefonici, gli indirizzi email del personale e degli studenti;
11. Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati;
12. Segnalare tempestivamente al proprio responsabile la presenza di documenti incustoditi, provvedendo temporaneamente alla loro custodia;
13. Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal proprio Responsabile o dal Titolare;
14. Conservare i supporti contenenti dati particolari in armadi chiusi, ad accesso controllato o in file protetti da password;
15. Non riutilizzare i supporti informatici utilizzati per il trattamento di dati sensibili per altri trattamenti;
16. Non gestire informazioni su più archivi ove non sia strettamente necessario e comunque curarne l'aggiornamento in modo organico

#### Altre istruzioni

1. Non comunicare e non diffondere dati e informazioni di natura personale o scolastici che non siano necessari per lo svolgimento delle attività amministrative per le quali si è incaricati;
2. Non comunicare né diffondere informazioni sullo stato di salute o comunque informazioni di natura particolare ex artt.9-10 del GDPR acquisite o comunque di cui si viene a conoscenza, al di fuori degli stretti obblighi di natura professionale;
3. Non realizzare e non diffondere foto, filmati, audio relativi alla vita scolastica o foto/video di documenti dei quali si viene in possesso;
4. Non comunicare e non diffondere informazioni riferite a specifici alunni, genitori, personali, a terzi, attraverso canali di comunicazione privata.

### **LINEE GUIDA IN MATERIA DI SICUREZZA PER IL COLLABORATORE SCOLASTICO INCARICATO DEL TRATTAMENTO**

Il collaboratore scolastico deve attenersi scrupolosamente alle suddette e alle seguenti indicazioni per garantire la sicurezza dei dati personali trattati:

1. Accertarsi che al termine delle lezioni non restino incustoditi i seguenti documenti, segnalandone tempestivamente la loro eventuale presenza al responsabile di sede e provvedendo temporaneamente alla custodia:
  - a. Di Certificati medici esibiti dagli alunni a giustificazione delle assenze;



b. Di Qualunque altro documento contenente dati personali o particolari degli alunni o dei docenti.

1. Accertarsi che al termine delle lezioni tutti i computer o i dispositivi usati per la didattica siano spenti e che non siano stati lasciati incustoditi supporti di memorizzazione (dispositivi USB, CD/DVD, ...), cartelle o altri materiali; in caso contrario, segnalarne tempestivamente la presenza al proprio responsabile provvedendo temporaneamente alla loro custodia.
2. Verificare la corretta funzionalità dei meccanismi di chiusura di armadi che custodiscono dati personali, segnalando tempestivamente al responsabile di sede eventuali anomalie.
3. Procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei locali siano state attivate.
4. Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati.
5. Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengano dati personali o sensibili, ma accertarsi che esse vengano sempre distrutte.
6. Non lasciare incustodito il registro contenente gli indirizzi, i recapiti telefonici, gli indirizzi email del personale.
7. Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati.
8. Non consentire che estranei possano accedere ai documenti dell'ufficio o leggere documenti contenenti dati personali o particolari.
9. Segnalare tempestivamente al proprio Responsabile la presenza di documenti incustoditi e provvedere temporaneamente alla loro custodia.
10. Procedere alla chiusura dei locali non utilizzati in caso di assenza del personale.
11. Procedere alla chiusura dei locali di segreteria accertandosi che siano state attivate tutte le misure di protezione e che le chiavi delle stanze siano depositate negli appositi contenitori.
12. Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal proprio Responsabile o dal Titolare.

#### Altre istruzioni

1. Non comunicare e non diffondere dati e informazioni di natura personale o scolastici che non siano necessari per lo svolgimento delle attività per le quali si è incaricati;
2. Non comunicare né diffondere informazioni sullo stato di salute o comunque informazioni di natura particolare ex artt.9-10 del GDPR acquisite o comunque di cui si viene a conoscenza, al di fuori degli stretti obblighi di natura professionale;
3. Non realizzare e non diffondere foto, filmati, audio relativi alla vita scolastica o foto/video di documenti dei quali si viene in possesso;
4. Non comunicare e non diffondere informazioni riferite a specifici alunni, genitori, personali, a terzi, attraverso canali di comunicazione privata.