MODELLO ORGANIZZATIVO DELL'ISTITUTO OMNICOMPRENSIVO "G.N. D'AGNILLO" IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI, IN APPLICAZIONE DEL REGOLAMENTO (UE) 2016/679 (GDPR).

Art. 1
Oggetto e ambito di applicazione

1. L'Istituto Omnicomprensivo "G.N. D'Agnillo" di Agnone è il Titolare del trattamento dei dati personali;
2. Il presente documento definisce un modello organizzativo in cui sono individuati i soggetti mediante i quali l'Istituto Omnicomprensivo "G.N. D'Agnillo" esercita le funzioni di Titolare del trattamento dei dati personali.
3. Le disposizioni contenute nel presente documento si applicano a tutte le strutture organizzative dell'Istituto Omnicomprensivo "G.N. D'Agnillo";
4. Il presente documento è consultabile nella sezione Privacy del sito internet dell'Istituto.

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 il DPO - RPD previsto dalla normativa;
    b. verificare la legittimità dei trattamenti di dati personali effettuati all'interno dell'Istituzione Scolastica;
    c. disporre, in conseguenza della verifica di cui alla lett. b., le modifiche necessarie ai trattamenti affinché gli stessi siano conformi alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
    d. verificare il costante aggiornamento del Registro delle attività di trattamento previsto dall'art. 30 del GDPR;
    e. garantire la corretta informazione agli interessati e il regolare esercizio dei loro diritti;
    f. verificare l'aggiornamento della modulistica, in coerenza con la normativa sulla Privacy;
    g. curare la formazione del personale dell'Istituzione Scolastica e fornire le necessarie istruzioni per il corretto trattamento dei dati personali;
    h. verificare che i soggetti autorizzati a compiere operazioni di trattamento operino, ai sensi del successivo articolo 4, nel rispetto delle istruzioni fornite per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;
    i. individuare i Responsabili esterni del trattamento e perfezionare gli atti previsti dall'art. 28 del GDPR;
    j. attivare, senza indugio, in caso di incidenti riguardanti la sicurezza dei dati (Data Breach) la Struttura di Coordinamento Privacy e collaborare con essa per la gestione dell'incidente;
    k. effettuare, nei casi previsti dall'art. 35 del GDPR, la Valutazione d'Impatto sulla protezione dei dati.

Art. 3
Struttura di Coordinamento Privacy

1. In assistenza al Titolare, è costituito un gruppo di gestione delle attività di trattamento dei dati personali diretto dal DSGA e costituito dal DSGA e dal Responsabile dell'Ufficio Tecnico e da due assistenti amministrativi;
2. 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'analisi dei rischi dei trattamenti e alla predisposizione delle necessarie misure di sicurezza;

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

Art. 4
Autorizzazione al trattamento

1. I dipendenti dell'Istituzione Scolastica (Docenti, Assistenti Amministrativi, Assistenti Tecnici, Collaboratori Scolastici) e i soggetti che operano ad altro titolo nell'ambito della stessa Istituzione sono autorizzati al trattamento dei dati personali gestiti dall'Istituzione Scolastica in base alle specifiche competenze, al ruolo, alle funzioni ed agli incarichi ricevuti e nel rispetto delle istruzioni generali e specifiche allegate al presente Modello.

IL DIRIGENTE SCOLASTICO
Dott.ssa Tonina Camperchioli

Allegato A - ISTRUZIONI GENERALI

ISTRUZIONI AGLI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali da parte degli autorizzati deve 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 dei dati 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 con modalità compatibili con tali scopi;
3. Verificare che i dati siano esatti e, se necessario, aggiornarli;
4. Verificare che i dati siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
5. Non comunicare a terzi i dati, al di fuori dell'ambito lavorativo o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
6. Accedere solo ai dati strettamente necessari per l'esercizio delle proprie mansioni;
7. 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

1. Conservare sempre i dati del cui trattamento si è incaricati in apposito armadio 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. Non consentire l'accesso a estranei ai fax 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 documenti inutilizzati che è necessario eliminare;
7. Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengano dati personali o sensibili, 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 trattati;
9. Segnalare tempestivamente al proprio responsabile la presenza di documenti incustoditi, provvedendo temporaneamente alla loro custodia;
10. Riguardo ai trattamenti eseguiti con supporto informatico, attenersi scrupolosamente alle seguenti indicazioni:

a. DATI E SUPPORTI INFORMATICI
    i. Non lasciare supporti di memorizzazione, cartelle o altri documenti a disposizione di estranei;
    ii. conservare i dati sensibili in armadi chiusi, ad accesso controllato o in files protetti da password;
    iii. non consentire l'accesso ai dati a soggetti non autorizzati;
    iv. riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi;
    v. non riutilizzare i supporti informatici utilizzati per il trattamento di dati sensibili per altri trattamenti.
b. PASSWORD
    i. Scegliere una password con le seguenti caratteristiche: originale, composta almeno da otto caratteri, che contenga almeno un numero, che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o alla propria professione facilmente ricostruibili:
    ii. curare la conservazione della propria password ed evitare di comunicarla ad altri;
    iii. cambiare periodicamente (almeno una volta ogni tre mesi) la propria password.
c. POSTAZIONE DI LAVORO
    i. Proteggere la propria postazione di lavoro con una password;
    ii. spegnere correttamente il computer al termine di ogni sessione di lavoro;
    iii. non lasciare incustodita la propria postazione di lavoro per la pausa o per altri motivi senza aver spento i computer o senza essersi disconnessi dalle sessioni attive e aver inserito uno screen saver con password;
    iv. comunicare tempestivamente, al proprio responsabile, qualunque anomalia riscontrata nel funzionamento del computer;
d. POSTA ELETTRONICA
    i. Non aprire documenti di cui non sia certa la provenienza;
    ii. non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus;
    iii. controllare accuratamente l'indirizzo dei destinatari prima di inviare dati personali.

ALL.B - ISTRUZIONI SPECIFICHE

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

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

A. Per il trattamento dei dati sui computer condivisi (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 dati personali (propri e di altre persone) sui computer;
   5. scegliere una password con le seguenti caratteristiche:
      a. originale;
      b. composta almeno da otto caratteri;
      c. che contenga almeno un numero;
      d. che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o professione facilmente ricostruibili.
   6. curare la conservazione della propria password ed evitare di comunicarla ad altri;
   7. cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
   8. modificare prontamente (ove possibile) la password assegnata;
   9. non lasciare incustodita la postazione di lavoro senza essersi disconnessi dalle sessioni attive o senza averla spento il proprio strumento di lavoro a fine giornata;
   10. utilizzare le seguenti regole per la posta elettronica:
      a. non aprire documenti di cui non sia certa la provenienza;
      b. non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus;
      c. controllare accuratamente l'indirizzo dei destinatari prima di inviare dati personali.

B. Per il trattamento dei dati in formato cartaceo seguire le seguenti istruzioni:
   1. Tutta la documentazione che contiene dati personali degli alunni deve essere custodita in un apposito armadio a cassetti, dotato di serratura, sito nella sala dei professori e la cui chiave non deve esser lasciata incustodita;
   2. ogni docente è responsabile della corretta tenuta del cassetto, della sua regolare chiusura e della segnalazione di ogni inconveniente che possa compromettere la custodia;
   3. 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;
   4. le prove personali degli alunni sono custodite nel cassetto personale e poi consegnate all'Ufficio di Segreteria che ne curerà la custodia.

ALL.C - ISTRUZIONI SPECIFICHE

LINEE GUIDA IN MATERIA DI SICUREZZA PER L'ASSISTENTE TECNICO INCARICATO DEL TRATTAMENTO

L'Assistente tecnico deve attenersi scrupolosamente alle seguenti indicazioni per garantire la sicurezza dei dati personali trattati:

A. Per il trattamento dei dati sui computer condivisi (Aula di informatica, 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 dati personali (propri e di altre persone) sui computer;
5. scegliere una password con le seguenti caratteristiche:
    a. originale;
    b. composta almeno da otto caratteri;
    c. che contenga almeno un numero;
    d. che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o professione facilmente ricostruibili.
6. curare la conservazione della propria password ed evitare di comunicarla ad altri;
7. cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
8. modificare prontamente (ove possibile) la password assegnata;
9. non lasciare incustodita la postazione di lavoro senza essersi disconnessi dalle sessioni attive o senza averla spento il proprio strumento di lavoro a fine giornata;
10. utilizzare le seguenti regole per la posta elettronica:
    a. non aprire documenti di cui non sia certa la provenienza;
    b. non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus;
    c. controllare accuratamente l'indirizzo dei destinatari prima di inviare dati personali.

B. Per il trattamento dei dati in formato cartaceo seguire le seguenti istruzioni:

a. Tutta la documentazione che contiene dati personali degli alunni deve essere custodita in un apposito armadio a cassetti, dotato di serratura, sito nella sala dei professori e la cui chiave non deve esser lasciata incustodita;

b. ogni assistente è responsabile della corretta tenuta dell'armadietto, della sua regolare chiusura e della segnalazione di ogni inconveniente che possa compromettere la custodia.

ALL.D - ISTRUZIONI SPECIFICHE

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

L'assistente amministrativo deve attenersi scrupolosamente 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 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 e alla stampante che contengano 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 sensibili, ma accertarsi che esse vengano sempre distrutte;
10. Non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici 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. Riguardo ai trattamenti eseguiti con supporto informatico, attenersi scrupolosamente alle seguenti indicazioni:

    <u>Dati e supporti informatici</u>

    a. Non lasciare supporti di memorizzazione, cartelle o altri documenti a disposizione di estranei;
    b. Conservare i dati sensibili in armadi chiusi, ad accesso controllato o in file protetti da password;
    c. Non consentire l'accesso ai dati a soggetti non autorizzati;
    d. Riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove essi sono custoditi;
    e. Non riutilizzare i supporti informatici utilizzati per il trattamento di dati sensibili per altri trattamenti;
    f. Non gestire informazioni su più archivi ove non sia strettamente necessario e comunque curarne l'aggiornamento in modo organico.

Password

a. Scegliere una password con le seguenti caratteristiche:
    i. originale
    ii. composta almeno da otto caratteri
    iii. che contenga almeno un numero
    iv. che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili;
b. Curare la conservazione della propria password ed evitare di comunicarla ad altri;
c. Cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
d. Per le password soggette a protezione da parte del Custode delle credenziali, trascrivere su un Modello chiuso in busta sigillata e controfirmata la nuova password e consegnarla al custode delle credenziali.

Postazione di lavoro

a. Proteggere la propria postazione di lavoro con una password;
b. Spegnere correttamente il computer al termine di ogni sessione di lavoro;
c. Non lasciare incustodita la propria postazione di lavoro per la pausa o altri motivi senza averla spento il computer o essersi disconnessi dalle sessioni attive e aver inserito uno screen saver con password;
d. Comunicare tempestivamente al Titolare o al proprio Responsabile qualunque anomalia riscontrata nel funzionamento del computer.

Posta elettronica

a. Utilizzare le seguenti regole per la posta elettronica:
    i. Non aprire documenti di cui non sia certa la provenienza;
    ii. Non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus;
    iii. Inviare messaggi di posta solo se espressamente autorizzati dal proprio Responsabile;
    iv. Controllare accuratamente l’indirizzo dei destinatari prima di inviare dati personali.

ALL.E - ISTRUZIONI SPECIFICHE

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

Il collaboratore scolastico deve attenersi scrupolosamente 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 loro custodia:
   a. Certificati medici esibiti dagli alunni a giustificazione delle assenze;
   b. Qualunque altro documento contenente dati personali o sensibili degli alunni o dei docenti.
2. Accertarsi che al termine delle lezioni tutti i computer 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.
3. Verificare la corretta funzionalità dei meccanismi di chiusura di armadi che custodiscono dati personali, segnalando tempestivamente al responsabile di sede eventuali anomalie.
4. Procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei locali siano state attivate.
5. Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati.
6. 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.
7. Non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici del personale.
8. Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati.
9. Non consentire che estranei possano accedere ai documenti dell'ufficio o leggere documenti contenenti dati personali o sensibili.
10. Segnalare tempestivamente al proprio Responsabile la presenza di documenti incustoditi e provvedere temporaneamente alla loro custodia.
11. Procedere alla chiusura dei locali non utilizzati in caso di assenza del personale.
12. 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.
13. Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal proprio Responsabile o dal Titolare.