



MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA

ISTITUTO COMPRENSIVO ALFANO – QUASIMODO

Via dei Mille, 41 – 84132 Salerno ☎ fax 089 334918

mail saic89300a@istruzione.it

pec saic89300a@pec.istruzione.it

sito www.icalfanoquasimodo.edu.it

C.M. SAIC89300A

C.F. 95121350656

C.U. UFV04C

C.IPA istsc_saic89300a

Prot. 1943

25.9.2020

AMMINISTRATIVI - DOCENTI – AUSILIARI
RESPONSABILE PROTEZIONE DATI SCUOLA
ALBO – AMMINISTRAZIONE TRASPARENTE

Oggetto: aggiornamento DPS – incarichi - informativa

DLgs 196/2003 (codice) - DM 305/2006 - Regolamento UE 2016/679 (regolamento)

PREMESSA

Il presente documento programmatico per la sicurezza dei dati personali (DPS) è stato redatto dal dirigente scolastico e sarà aggiornato a seguito dell'evoluzione del "modello organizzativo della privacy" di questa Scuola e/o dell'entrata in vigore di nuove norme.

L'articolazione è quella prevista al punto 19 dell'allegato B al "codice":

1. elenco dei trattamenti di dati personali
2. distribuzione di compiti e responsabilità in ordine ai trattamenti
3. analisi dei rischi che incombono sui dati personali trattati dalla scuola
4. misure per garantire integrità e disponibilità dei dati e protezione dei locali
5. criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento
6. interventi formativi degli incaricati del trattamento, per renderli edotti sui rischi che incombono sui dati
7. criteri da adottare per i trattamenti di dati personali affidati all'esterno dell'istituzione scolastica
8. criteri da adottare per la cifratura o la separazione di dati sensibili idonei a rivelare lo stato di salute
9. ulteriori misure in caso di trattamento di dati sensibili o giudiziari
10. misure attuative del documento programmatico per la sicurezza.

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

I dati personali, comuni e sensibili, trattati a Scuola riguardano essenzialmente gli allievi e il personale.

Ai sensi del dm 305/2006 è consentito il trattamento dei seguenti dati:

- selezione/reclutamento del personale
- gestione del contenzioso e dei procedimenti disciplinari
- organi collegiali e commissioni istituzionali
- attività propedeutiche all'avvio dell'anno scolastico
- attività educativa, didattica, formativa e di valutazione
- rapporti scuola/famiglie degli allievi.

Dati trattati dai docenti

I dati personali trattati dai docenti sono contenuti in banche dati su supporto cartaceo e informatizzato che si possono classificare in:

- dati ai quali hanno accesso più docenti
- dati ai quali ha accesso un singolo docente.

Le banche dati cui hanno accesso più docenti sono:

- A. il registro di classe e i verbali dei consigli d'intersezione/interclasse/classe

- B. la documentazione relativa alla programmazione didattica
- C. gli elaborati e i documenti di valutazione
- D. la documentazione dello stato di handicap
- E. i certificati medici degli allievi
- F. la corrispondenza con le famiglie degli allievi.

Le banche dati cui ha accesso il singolo docente sono:

- G. il registro personale/giornale dell'insegnante.

Dati trattati dal dirigente scolastico:

- a. atti riservati
- b. certificazioni di handicap
- c. documentazione didattica
- d. registro degli infortuni
- e. verbali degli organi collegiali
- f. comunicazioni dei genitori degli allievi.

Dati trattati dal DSGA:

- g. anagrafe fornitori
- h. documenti contabili
- i. contratti e convenzioni
- j. fascicoli relativi ad allievi infanzia/primaria/secondaria
- k. fascicoli relativi a tutto il personale scolastico
- l. richieste/comunicazioni personale/utenza.

Dati trattati dal personale amministrativo:

dalla lettera "b" alla lettera "l".

Dati trattati dal personale ausiliario:

lettera "f".

2. DISTRIBUZIONE DI COMPITI E RESPONSABILITÀ IN ORDINE AI TRATTAMENTI

Il Codice all'art. 4 individua le quattro figure coinvolte nel trattamento dei dati personali:

Il titolare è la persona fisica o giuridica che ha la responsabilità finale e assume le decisioni riferite al trattamento dei dati personali, quindi l'Istituzione scolastica, rappresentata dal dirigente pro-tempore.

Il responsabile è la persona, dotata di particolari caratteristiche di natura morale e di competenza tecnica, preposta dal titolare al trattamento dei dati personali ivi compreso il profilo della sicurezza. Per l'individuazione del responsabile, la cui nomina è facoltativa, esistono diverse possibilità:

- (1) non viene nominato, per cui il dirigente scolastico assume personalmente tutte le incombenze relative agli adempimenti previsti dal codice e provvedimenti collegati;
- (2) viene nominato il direttore dei servizi generali ed amministrativi per il trattamento dei dati che riguardano, in modo specifico, i servizi di segreteria, mentre il capo d'istituto si occupa direttamente del trattamento dei dati effettuato dai docenti;
- (3) vengono nominati il direttore dei servizi generali ed amministrativi per i trattamenti dei dati che riguardano in modo specifico i servizi di segreteria e uno o più docenti per il trattamento di dati effettuato dagli insegnanti per fini didattici.

In base a quanto disposto dall'articolo 29, comma 2 del "codice" (... *Il responsabile, se designato, deve essere nominato fra i soggetti che per esperienza capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza*...) si è deciso di adottare la soluzione illustrata al punto tre.

Gli incaricati sono le persone fisiche che materialmente provvedono al trattamento dei dati, secondo le istruzioni impartite dal titolare o dal responsabile: docenti, assistenti amministrativi, collaboratori scolastici, personale supplente temporaneo e, per quanto riguarda i trattamenti effettuati con strumenti elettronici, personale esterno incaricato della manutenzione.

Sono nominati incaricati del trattamento dei dati personali, ciascuno per la propria sfera di competenza, con atto che elenca puntualmente: categorie dei dati ai quali si ha accesso, tipologia di trattamento e vincoli specifici delle varie tipologie di dati, istruzioni in merito ai soggetti cui i dati possono essere comunicati.

L'interessato è il soggetto cui i dati trattati si riferiscono, la persona che ha diritto a ricevere l'informativa prevista all'art. del 13 del "codice" e che, salvo i casi di esclusione normativamente previsti, deve prestare il consenso al trattamento dei propri dati.

L'amministratore di sistema è la figura introdotta dal D.P.R. 318/99 art. 1, con il compito di "sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base di dati e consentirne l'utilizzazione". Nel "Codice" detta figura non viene inserita tra i soggetti coinvolti nel trattamento dei dati personali. In considerazione delle procedure semplificate, previste dai sistemi applicativi utilizzati dalla scuola (AXIOS/ARGO), si ritiene che tale funzione possa essere assolta dal direttore dei servizi generali e amministrativi in possesso di idonei requisiti.

Il trattamento dei dati

Gli amministrativi e i docenti trattano dati cartacei e informatici.

I docenti utilizzano registri personali e di classe elettronici. Le banche dati informatiche e cartacee contenenti documentazione didattica e personale vengono, a fine anno scolastico, consegnate dai docenti e custodite dal personale di segreteria. I locali dove avviene il trattamento dei dati effettuato dai docenti coincidono con quelli adibiti ad attività didattica, allocati nei plessi dell'istituzione scolastica.

Gli elaborati degli allievi, in quanto documenti che possono contenere dati personali, sono custoditi dai docenti e alla fine di ogni anno scolastico sono consegnati dai docenti alle famiglie degli allievi o in segreteria. Le certificazioni degli allievi e gli atti contabili sono custoditi in segreteria in locali e armadi chiusi, perché contengono sempre dati personali e spesso dati sensibili.

La situazione nelle sedi, caratteri comuni:

- modesta sicurezza delle porte d'ingresso e serrature ordinarie
- presenza di numerose vie di accesso e finestre non protette
- mancanza del sistema di allarme, ad eccezione dei plessi Alfano e S. Eustachio primaria, armadietti di classe provvisti di serratura.

3. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI PERSONALI TRATTATI DALLA SCUOLA

Si mettono di seguito in evidenza i rischi connessi al trattamento dei dati personali:

- non integrità dei dati
- distruzione o perdita di dati
- accesso non autorizzato ai dati
- reimpiego di supporti di memorizzazione
- utilizzo di reti di telecomunicazione disponibili al pubblico
- luoghi impropri di conservazione della documentazione relativa al trattamento
- trattamento di dati personali non consentito o non conforme alla finalità della raccolta.

Rischi riguardanti dati trattati senza l'ausilio di strumenti elettronici

Si riportano di seguito le possibili cause:

- distruzione o perdita accidentale dei dati a causa di eventi naturali e no
- accesso ai dati da parte di soggetti esterni o soggetti interni non autorizzati
- trattamento non consentito o non conforme alle finalità di raccolta, diffusione, comunicazione
- utilizzo di modalità di trattamento inadeguate o manomissioni che determinano non integrità dei dati.

Rischi riguardanti dati trattati con l'ausilio di strumenti elettronici

Si riportano gli elementi del sistema informatico automatizzato (SIA) che necessitano di protezione:

rete	Unica per i client e il server
tipologia rete	ADSL CONVERGENZE SPA
accesso ad internet	sì da tutti i p.c.
accesso posta elettronica	sì da tutti i p.c.
uso della rete	Condivisione documenti e archivi AXIOS e ARGO
n. 10 pc	segreteria in rete
sistema operativo	Client: WINDOWS 7 PRO – Server: Windows Server 2008
programmi	Microsoft Office, AXIOS, ARGO, Acrobat Reader, Zip
casella posta ministeriale	saic89300a@istruzione.it
personale	formazione annuale per tutto il personale
password	accesso alle singole macchine (Dominio Microsoft)
dati	backup effettuato in automatico periodicamente su supporto esterno (NAS)
registro dei backup	a cura del direttore dei servizi generali e amministrativi
gruppo di continuità	su tutti i computer degli uffici e sul Server

S'illustrano di seguito le possibili minacce al SIA:

- Hardware difetti produzione, usura, eventi naturali, uso improprio, furto, virus...
- Software difetti di produzione, errore, uso improprio, furto, intercettazione, virus
- Dati accesso non autorizzato e/o modifiche deliberate o accidentali
- Supporti memorizzazione distruzione/alterazione per eventi naturali, azioni accidentali/intenzionali deterioramento, inaffidabilità del mezzo fisico, evoluzione tecnologica
- Addetti a manutenzione attacchi al sistema, uso improprio per errore, uso improprio intenzionale.

4. MISURE PER GARANTIRE INTEGRITÀ E DISPONIBILITÀ DEI DATI E PROTEZIONE DEI LOCALI

Per individuare le misure di prevenzione da adottare in relazione ai rischi sopra rilevati è stato necessario analizzare la situazione logistica organizzativa degli edifici scolastici dove sono trattati dati personali.

I plessi Alfano - Quasimodo e S. Eustachio sono dotati di sistema d'allarme. L'accesso ai cortili è protetto da cancelli non elettrificati, quello agli edifici da porte metallo/vetro con serratura.

Per assicurare l'integrità e la disponibilità dei dati sono stati realizzati molti adeguamenti e sono stati programmati alcuni ulteriori interventi, si riporta, di seguito, un sintetico quadro della situazione articolata sulla base delle diverse tipologie di sicurezza da garantire:

SICUREZZA FISICA DI AREA

Deve prevenire accessi fisici non autorizzati, danni/interferenze con lo svolgimento dei servizi.

Adeguamenti realizzati

- a. nell'archivio, protetto dalla chiusura della doppia porta, custodia di copie di sicurezza di tutte le chiavi
- b. consegna chiavi armadi e scrivanie dove sono custodite le banche dati agli assistenti amministrativi
- c. costituzione di due distinti uffici: area del personale/allievi e protocollo/sportello
- d. sistemazione degli archivi, storico al piano terra e corrente nell'area uffici
- e. condivisione collegiale di tempi/modi di verifica/autovalutazione nelle sedute degli OOCC.

SICUREZZA FISICA DELLE APPARECCHIATURE

È riconducibile alle protezioni da danni accidentali/intenzionali e alla sicurezza degli impianti di alimentazione.

Adeguamenti realizzati

- a) aggiornamento annuale sull'importanza del rispetto delle norme di sicurezza
- b) contratto di assistenza/manutenzione hardware/software con ditta esterna
- c) differenziazione attività di formazione docenti e ata
- a) condivisione collegiale di tempi/modi di verifica/autovalutazione.

SICUREZZA FISICA DEGLI ARCHIVI

È garantita dalla presenza di porte, armadi e cassette con serratura efficiente nei locali in cui si trattano dati.

Adeguamenti realizzati: acquisto di nuove cassette e chiusura dei locali amministrativi tutte le volte che siano incustoditi, divieto di accesso alle aree dove sono custoditi i dati personali ai non addetti al trattamento, condivisione collegiale di tempi/modi di verifica/autovalutazione.

Da realizzare: acquisto di nuovi arredi in sostituzione di quelli privi di serrature.

SICUREZZA INFORMATICA

Riguarda principalmente la protezione di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento e utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo.

Per il SIDI (sistema informativo ministeriale) sono garantite le seguenti procedure di sicurezza:

- identificazione, ovvero riconoscimento personale di ogni utente e validazione dell'identità mediante assegnazione di codice d'identificazione e password (P.I.N.) per accesso al sistema, da tenere segreta;
- autorizzazione, ovvero determinazione delle azioni che ciascun utente è abilitato ad eseguire.

Adeguamenti realizzati: dotazione di un gruppo di continuità per ogni computer per eventuali black-out della rete elettrica, attribuzione d'incarico al DSGA di compilazione della lista incaricati e compiti agli amministrativi per il trattamento, manuale e informatico dei dati personali, redazione del regolamento per l'uso dei laboratori informatici da parte dei docenti, definizione, nel contratto di assistenza/manutenzione hardware/software, condivisione collegiale di tempi/modi di verifica/autovalutazione.

SICUREZZA ORGANIZZATIVA

Accanto all'adozione delle misure tecnologiche già illustrate, sono state definite norme e procedure per regolamentare gli aspetti organizzativi del processo di sicurezza.

Adeguamenti realizzati: incarichi al personale e istruzioni per l'espletamento dell'incarico e condivisione collegiale di tempi/modi di verifica/autovalutazione.

5. CRITERI E MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

Il responsabile, in caso di eventi che provochino la distruzione o il danneggiamento dei dati personali contenuti nelle banche dati del sistema informatico, provvederà senza ritardo a ripristinare la funzionalità delle banche dati utilizzando le copie di back-up.

6. INTERVENTI FORMATIVI DEGLI INCARICATI DEL TRATTAMENTO

Il titolare assicura in ogni anno scolastico, al responsabile e a tutti gli incaricati del trattamento di dati personali, un intervento di formazione quantificato in tre ore con modalità e-learning.

Gli argomenti da sviluppare sono relativi ai contenuti del codice:

- doveri dei lavoratori e degli incaricati
- responsabilità e compiti da svolgere in relazione alle misure adottate dal titolare
- profili della disciplina sulla protezione dei dati personali in rapporto alle specifiche attività.

Le ore di formazione sopra indicate, rientrando negli obblighi di servizio del personale, devono essere:

- svolte in orario di servizio, senza oneri aggiuntivi per il personale
- inserite nel piano annuale delle attività deliberato dagli oo.cc. di ciascun profilo professionale.

Per la partecipazione alle attività formative è previsto il rilascio di un attestato da inserire nel fascicolo.

7. CRITERI DA ADOTTARE PER I TRATTAMENTI DI DATI PERSONALI AFFIDATI ALL'ESTERNO

Allo stato attuale non sono state affidate a soggetti esterni, persone fisiche o giuridiche, attività che comportino trattamento di dati personali; se dovesse ravvisarsi tale necessità sarebbe osservata la seguente procedura:

- ▶ conferimento incarico per il trattamento dei dati con indicazione delle norme di comportamento;
- ▶ verifica periodica della correttezza del trattamento, con particolare riferimento all'adozione delle misure minime di sicurezza, da parte degli incaricati;
- ▶ richiesta di dichiarazione di conformità a quanto stabilito dalle norme di legge e dal presente documento.

8. CRITERI DA ADOTTARE PER CIFRATURA/SEPARAZIONE DI DATI SENSIBILI SU STATO DI SALUTE

Questa Istituzione tratta dati idonei a rivelare lo stato di salute del personale, docente e ATA, nonché degli allievi, esclusivamente per finalità previste dalla legge.

Secondo quanto prescritto dall'articolo 22 comma 7 del "Codice" ... *I dati idonei a rivelare lo stato di salute ... sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici; in questo caso, dunque, in base al comma 6 dell'art. 22 "... sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità".*

I dati riguardanti il personale docente e ATA (essenzialmente certificati medici) devono essere consegnati all'ufficio di segreteria, dopo il trattamento sono inseriti in una cartella da custodire nel fascicolo.

I dati riguardanti gli allievi (essenzialmente attestazioni di handicap e certificati medici) devono essere consegnati all'ufficio di segreteria, dopo il trattamento sono inseriti in una cartella da custodire nel fascicolo.

9. ULTERIORI MISURE IN CASO DI TRATTAMENTO DI DATI SENSIBILI O GIUDIZIARI

Nelle sette schede che costituiscono parte integrante del "Regolamento" il Ministero illustra i dati sensibili e giudiziari trattati dalle istituzioni scolastiche, definendo per ciascuna tipologia:

le fonti normative, le operazioni possibili, le finalità di rilevante interesse pubblico da perseguire.

Si riporta, di seguito lo schema di sintesi delle sette schede:

- a) scheda 1 (trattamento dati relativi a selezione, reclutamento e gestione del rapporto di lavoro)
- b) scheda 2 (dati sensibili e giudiziari connessi a contenziosi e gestione di affari penali e civili)
- c) scheda 3 (dati sensibili relativi all'appartenenza alle organizzazioni sindacali)
- d) scheda 4 (dati relativi ad allievi e famiglie per attività di avvio dell'anno scolastico)
- e) scheda 5 (dati nell'espletamento di attività curricolari, extracurricolari e di valutazione degli allievi)
- f) scheda 6 (dati connessi alle procedure di accreditamento e autorizzazione delle scuole non statali)
- g) scheda 7 (dati relativi ad attività connesse all'instaurazione di contenzioso con allievi e famiglie).

Per il trattamento dei dati indicati nelle schede succitate sono state adottate le seguenti misure:

- ▶ individuazione dei responsabili del procedimento di specifiche aree d'intervento: personale, allievi, protocollo, magazzino, contabilità
- ▶ definizione di modalità operative e vincoli per l'espletamento dell'incarico
- ▶ effettuazione di controlli periodici per verificare il rispetto delle procedure concordate.

10. MISURE ATTUATIVE DEL DOCUMENTO PROGRAMMATICO PER LA SICUREZZA

Annualmente si effettuano le seguenti azioni:

a cura del TITOLARE

aggiornamento DPS; nomina e istruzioni al responsabile/amministratore di sistema e agli incaricati del trattamento dati personali; informativa per tutto il personale, l'utenza e soggetti esterni; stipula dei contratti per informazione annuale del personale e assistenza hardware e software;

a cura del RESPONSABILE

redazione lista incaricati di trattamento con e senza l'ausilio di strumenti elettronici; consegna delle chiavi edifici e antifurti al personale scolastico e a quello della ditta di pulizia esterna; aggiornamento delle tabelle relative a computer uffici e password di ciascun computer, locali, arredi e dati in essi custoditi; attribuzione di compiti per il trattamento manuale e informatico dei dati personali, la protezione/aggiornamento dai virus, il back-up periodico e l'annotazione dei salvataggi su registro all'uso istituito; controllo di accesso alle macchine e identificazione degli utenti attraverso password; verifiche esigenze per migliorare la custodia dei dati da inoltrare al Comune o da programmare nel PA.

ALLEGATI:

- informativa prevista dall'art. 13 del DLgs 196/2003 e dall'art. 13 del Regolamento UE 2016/679
- nomina del Responsabile del trattamento dei dati personali e amministratore di sistema
- nomina degli incaricati del trattamento dei dati personali
- istruzioni

IL DIRIGENTE SCOLASTICO
Giuseppina Del Giudice

*Firma autografa sostituita a mezzo stampa
ai sensi e per gli effetti dell'art. 3 c. 2 D. Lgs. n. 39/93*