I.C. PICERNO - PZ
Prot. N. ...5353.....
DEL ....07/12/2023...

Sommario

1.0 Scopo della procedura 3
2.0 Campo di applicazione della procedura 3
3.0 Abbreviazioni 3
4.0 Riferimenti 4
5.0 Modalità operative di tutela dei dati personali e misure di sicurezza 5
5.1 - Regole generali 6
5.2 - Trattamenti dei dati personali su supporto cartaceo 7
5.2.1 Procedura di Protezione Dati: documenti in ingresso 7
5.2.2 Procedura di Protezione Dati: documenti in uscita 7
5.2.3 Procedura di Protezione Dati: verifica della legittimità del trattamento in corso 7
5.2.4 Procedura di Protezione Dati: quando un alunno o un dipendente ci lascia definitivamente 8
5.2.5 Procedura di Protezione Dati: classificazione immediata di ogni documento/protocollo 8
5.2.6 Procedura di Protezione Dati: circoscrivere al massimo il numero di Autorizzati che trattano una pratica 8
5.2.7 Procedura di Protezione Dati: affidamento all'Autorizzato sotto la sua responsabilità 8
5.2.8 Procedura di Protezione Dati: custodia separata per i dati relativi allo stato di salute 9
5.2.9 Procedura di Protezione Dati: Regole generali per la sicurezza degli archivi 9
5.2.10 Procedura di Protezione Dati: archiviazione nel fascicolo personale 11
5.2.11 Procedura di Protezione Dati: archiviazione nell'archivio storico 11
5.2.12 Procedura di Protezione Dati: scarto periodico dei documenti 11
5.2.13 Procedura di Protezione Dati: distruzione dei documenti 11
5.2.14 Procedura di Protezione Dati: appunti, bozze e copie superflue 11
5.2.15 Procedura di Protezione Dati: cautele nella fase di fotocopiatura 11
5.2.16 Procedura di Protezione Dati: la movimentazione da parte di terzi 12
5.2.17 Procedura di Protezione Dati: pulizia dei locali contenenti archivi 12
5.2.18 Procedura di Protezione Dati: ingresso di persone esterne per manutenzione 12
5.2.19 Procedura di Protezione Dati: ingresso di altre persone in segreteria 12
5.3 - Trattamenti con strumenti elettronici – documenti informatici o digitali 12
6 - Trattamenti da parte dei docenti 17
6.1 Procedura di Protezione Dati: registri 17
6.2 Procedura di Protezione Dati: certificazioni mediche e informazioni sullo stato di salute degli alunni 17

0		Prima revisione			
Rev.	***Data***	***Descrizione revisione***	***Redazione*** (RPD):ing. A. Di Bitonto	***Emissione*** (DSGA): Dir.L. Babsia	***Approvazione*** (DS): prof. V. Vasti

6.3 Procedura di Protezione Dati: elaborati contenenti notizie particolari 17

6.4 Procedura di Protezione Dati: gestione degli elenchi degli alunni 18

6.5 Procedura di Protezione Dati: gestione di documenti scolastici 18

7 - Trattamenti da parte dei Collaboratori Scolastici e del Personale Ausiliario 18

7.1 Procedura di Protezione Dati: gestione di documenti scolastici 18

7.2 Procedura di Protezione Dati: trasporto di documenti scolastici 19

7.3 Procedura di Protezione Dati: custodia 19

8 – L'Amministratore di Sistema 19

9 – Il Data Breach (Violazione dei dati personali) 20

1.0 Scopo della procedura

Il presente documento è finalizzato a delineare l'insieme delle misure di sicurezza, organizzative, fisiche, logistiche e logiche, da adottare per il trattamento dei dati personali effettuato dal seguente Titolare: IC di Picerno (PZ).

2.0 Campo di applicazione della procedura

La procedura riguarda le misure di sicurezza da adottare per il trattamento dati personali sia che siano contenuti su supporti cartacei che su supporti digitali.
La presente procedura si applica considerato che tutte le correnti disposizioni ministeriali e norme sul flusso documentale, riportate al successivo paragrafo 4, siano attuate o in fase di attuazione.
In particolare le procedure della corretta gestione dei dati sono riportate nel "**Manuale dei flussi documentali**" adottato dall'Istituto, nella sua revisione corrente.
La presente procedura riporta in dettaglio le procedure di sicurezza da adottare ai flussi documentali gestiti come richiamato dal suddetto manuale al paragrafo 6.1.

3.0 Abbreviazioni

DS	= Dirigente Scolastico / Rappresentante legale del Titolare del trattamento dati: IC di Picerno (PZ)
DSGA	= Direttore dei Servizi Generali ed Amministrativi
RPD	= Responsabile della Protezione dei Dati (DPO)
AmS	= Amministratore di Sistema
ASA	= Addetto ai Servizi Amministrativi designato dal DSGA
Rweb	= Responsabile Sito web istituzionale
RTD	= Responsabile Trattamento Dati
RGPD	= Regolamento sulla Protezione dei Dati Personali - UE 679/2016 –
AgID	= Agenzia per l'Italia Digitale
CAD	= Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005 e ss.mm.ii.)
PP	= Procedura della Privacy

4.0 Riferimenti

I principali riferimenti sono:

D.P.R. 445/2000 e successive modificazioni	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA)
D.Lgs. 42/2004 e successive modificazioni	Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137[1]
Linee Guida AgID	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, adottate dall'AgID con Determinazione n. 407/2020 del 9 settembre 2020 ed in seguito aggiornate con Determinazione n. 371/2021 del 17 maggio 2021 (da attuare entro il 1° gennaio 2022)
L. 241/1990	Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi
D.Lgs. 196/2003 e successive modificazioni	Codice in materia di protezione dei dati personali
D.Lgs. 82/2005 e successive modificazioni	Codice dell'amministrazione digitale (CAD)
DPCM del 22 febbraio 2013	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71
DPCM del 21 marzo 2013	Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni
Regolamento UE 910/2014 (Regolamento *eIDAS*)	Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

In particolare si fa riferimento al paragrafo 6.1 dei "Manuale dei flussi documentali" dell'IC Picerno (PZ)

5.0 Modalità operative di tutela dei dati personali e misure di sicurezza

Il sistema di gestione documentale dell'Istituzione scolastica adotta un meccanismo di *compliance* e rispetto della normativa in materia di protezione dei dati personali, ai sensi del Reg. UE 679/2016 e del D.Lgs. 196/2003, modificato dal D.Lgs. 101/2018.

L'Istituzione scolastica adotta iniziative volte ad ottemperare a quanto previsto dal Regolamento UE 679/2016, con particolare riferimento:

- al principio di liceità del trattamento dei dati;
- al principio di minimizzazione del trattamento dei dati;
- all'esercizio dei diritti di cui agli artt. 15-22 del GDPR da parte degli interessati;
- alle modalità del trattamento e ai requisiti dei dati;
- all'informativa fornita agli interessati ed al relativo consenso quando dovuto;
- all'analisi dei rischi sui diritti e le libertà dei soggetti interessati;
- all'individuazione del Responsabile della protezione dei dati;
- all'individuazione dei Soggetti autorizzati al trattamento dei dati;
- all'analisi dei rischi sui diritti e le libertà dei soggetti interessati;
- alle misure di sicurezza.

L'Istituzione scolastica adottare le preventive misure di sicurezza, volte a custodire i dati personali trattati, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Nello specifico, le misure di carattere tecnico/organizzativo adottate dall'Istituzione scolastica sono le seguenti: [*elenco delle misure adottate*].

[Le misure di carattere tecnico/organizzativo possono comprendere, se del caso e a titolo esemplificativo:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.]

5.1 - Regole generali

Categorie di autorizzati: tutte

Principi di sicurezza

I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Il **DSGA** sentito l'**AmS** e il **RPD** si aggiorna e forma il personale sull'adozione delle nuove procedure di sicurezza adottate.

Documenti informatici o digitalizzati

Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate le seguenti misure minime:

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli Autorizzati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

L'**AmS** verifica periodicamente l'adozione di tali misure.

Documenti cartacei

Il trattamento di dati personali su supporto cartaceo è consentito solo se sono adottate, le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli Autorizzati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli Autorizzati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli Autorizzati.

Il **DSGA** vigila sull'adozione di tali misure.

5.2 - Trattamenti dei dati personali su supporto cartaceo

Categorie di Autorizzati: Assistenti Amministrativi, DSGA, Collaboratori Scolastici per quanto di loro pertinenza

5.2.1 Procedura di Protezione Dati: documenti in ingresso

I documenti in ingresso sono i documenti o i supporti contenenti dati personali acquisiti dalla scuola ai fini di un loro impiego in trattamento.

Per quanto attiene al trattamento dei documenti in ingresso, è necessario adottare le seguenti cautele:

a) i documenti in ingresso devono essere utilizzati soltanto da chi sia autorizzato al trattamento dei dati che contengono (cfr. documento di autorizzazione docenti, collaboratori e amministrativi);
b) l'autorizzato, ognuno per le proprie mansioni deve verificare:
c) la provenienza dei documenti;
d) che tali documenti siano effettivamente necessari al trattamento in questione;
e) la tipologia dei dati contenuti (comuni, particolari: giudiziari o sensibili), al fine di individuare le modalità legittime ed idonee per il trattamento e le misure di sicurezza da attuare;
f) l'osservanza del principio di pertinenza e non eccedenza rispetto o alle finalità del trattamento, la completezza, la correttezza e l'aggiornamento dei dati;

5.2.1.1 Procedura di Protezione Dati: informativa per la raccolta di dati personali

Ogni raccolta di dati personali dev'essere accompagnata dalla sottoscrizione per attestazione della presa visione dell'apposita informativa di cui all'art. 13 del Reg. UE 679/2016, fornita dal Titolare su supporto cartaceo, solo se l'interessato non può visionarla dal sito web istituzionale o ricevere da piattaforma gestionale (ARGO, Spaggiari e similari).

L'informativa cartacea è da inserire obbligatoriamente in tutte le dichiarazioni sostitutive di certificazione e di atto notorio:

Ai sensi dell'art. 48 del D. P. R. n. 445 del 28 dicembre 2000 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), è obbligatorio inserire l'informativa nella modulistica per la presentazione delle dichiarazioni sostitutive di certificazione e di atto notorio.

5.2.2 Procedura di Protezione Dati: documenti in uscita

Per "documenti in uscita", si intendono i documenti o i supporti contenenti dati personali prodotti e rilasciati dalla scuola a soggetti esterni ad essa.

L'Autorizzato del trattamento deve trattare qualunque prodotto dell'elaborazione di dati personali, ancorché non costituente documento definitivo, (appunti, stampe interrotte, stampe di prova, stampe elaborazioni temporanee ecc.) con le stesse cautele che sarebbero riservate alla a versione definitiva (v. misure relative ai trattamenti informatizzati).

Nel caso di documenti in uscita è necessario all'atto della consegna o dell'invio, verificare che la persona che riceve il documento sia legittimata al ritiro e all'utilizzo.

5.2.3 Procedura di Protezione Dati: verifica della legittimità del trattamento in corso

Di fronte a qualsiasi nuovo trattamento di dati, l'Autorizzato deve chiedersi se rientra nel preciso recinto di legittimità, delimitato dai seguenti paletti:

Il trattamento sia connesso con l'esercizio delle funzioni istituzionali (principio di pertinenza) e che esse non siano perseguibili attraverso il trattamento di dati anonimi.

Le modalità del trattamento siano tali da determinare il minimo sacrificio possibile del diritto alla riservatezza dell'Interessato (principio di non eccedenza: è illegittimo chiedere un dato in più di quello che è strettamente necessario).

Ogni fase del trattamento rispetti le norme di legge e di regolamento.

In ogni fase del trattamento siano adottate le misure di sicurezza previste per la categoria alla quale il dato appartiene

Se il dato è sensibile o giudiziario, siano rispettati i presupposti per avere la legittimazione a trattarlo

In caso di comunicazione o diffusione, che il dato rientri nelle categorie autorizzate

5.2.4 Procedura di Protezione Dati: quando un alunno o un dipendente ci lascia definitivamente

Gli vanno consegnati tutti i documenti contenenti dati personali che la scuola non sia obbligata a conservare. Nel caso non fosse possibile trattare direttamente con l'Interessato, si deve mandare un avviso per il ritiro. Nel frattempo i materiali da consegnare vanno posti in busta chiusa. Al ritiro va fatta firmare una ricevuta. Se passato un lasso ragionevole di tempo, l'interessato un suo delegato non si presenterà a ritirarli, si avvierà una procedura di distruzione dei documenti, con apposito verbale, ovviamente valutando prima se ci sono documenti che non sia opportuno eliminare (ad esempio, diplomi originali e simili).

In ogni caso qualunque fascicolo personale che transiti dall'archivio corrente a quello storico, dev'essere prima depurato di tutti dati personali non più necessari.

5.2.5 Procedura di Protezione Dati: classificazione immediata di ogni documento/protocollo

Non appena qualsiasi Autorizzato si accorge che un documento contiene dati personali di livello superiore a "comune" o "anonimo" deve scrivere in matita sull'angolo destro superiore del foglio la sigla descrivente il tipo di dato: "P" = dato particolare.

L'Autorizzato che riceve "brevi manu" allo sportello o in qualsiasi altro punto della scuola documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza o con sigla "P" ancora non collocati in busta chiusa, deve immediatamente metterli in busta chiusa e inserirli nella posta in arrivo per il Dirigente Scolastico.

5.2.6 Procedura di Protezione Dati: circoscrivere al massimo il numero di Autorizzati che trattano una pratica

I documenti contenenti dati personali di tipo sensibile, giudiziario o ad alto livello di delicatezza devono essere visti e conosciuti dal minor numero possibile di Autorizzati. Le pratiche relative a tali documenti devono essere seguite nell'intero iter possibilmente da una sola persona (compresa la fase di protocollo), salvo diversa disposizione del Dirigente.

5.2.7 Procedura di Protezione Dati: affidamento all'Autorizzato sotto la sua responsabilità

In generale qualsiasi documento o fascicolo contenente dati personali va trattenuto dall'Autorizzato per il tempo strettamente necessario alla lavorazione e riposto nel suo archivio appena terminato il lavoro o alla fine della giornata lavorativa. Non devono essere lasciati sui tavoli o comunque fuori dai contenitori documenti o fascicoli contenenti dati personali.

Nei casi in cui i documenti con dati particolari debbano essere trattati per un certo periodo di tempo, vengono mantenuti sotto la responsabilità dell'Autorizzato per il più breve tempo possibile. L'Autorizzato ha istruzione di elaborare le pratiche riferite a questi documenti in una stanza chiusa, ad accesso riservato almeno in quel momento, in modo che nessun altro possa sbirciarli o tanto meno trovarli momentaneamente abbandonati sul tavolo; nei momenti di non utilizzazione di conservarli dentro un cassetto o un armadio chiuso a chiave, del quale soltanto l'Autorizzato ha la chiave.

5.2.8 Procedura di Protezione Dati: custodia separata per i dati relativi allo stato di salute

Per dati relativi allo stato di salute ed alle abitudini sessuali (omosessualità, reati di tipo sessuale, ecc.) c'è l'obbligo di custodia separata rispetto agli altri dati trattati per finalità che non richiedono il loro utilizzo.

5.2.9 Procedura di Protezione Dati: Regole generali per la sicurezza degli archivi

Vanno poste in essere le misure necessarie a ridurre al minimo i rischi di:

a) accesso fisico non autorizzato;
b) furto o manomissione dei dati da parte di malintenzionati; distruzione o perdita dei dati dovuta ad eventi fisici;
c) perdita accidentale dei dati.

Gli archivi possono essere soltanto di due tipi:
- **a bassa sicurezza**, per dati comuni o neutri, con accesso "selezionato" (= il DS o il DSGA decidono chi può entrarvi e gli danno la chiave personale o mettono a disposizione la chiave in modo che solo costoro possono utilizzarla). È fondamentale assicurarsi che esista un numero definito di chiavi e che la chiave di riserva sia chiusa in luogo ben protetto. È stato nominato con atto formale un Autorizzato "Responsabile delle chiavi" che deve controllare.
- **Ad alta sicurezza**, ovviamente per dati sensibili o giudiziari, con accesso non solo selezionato, ma anche "controllato": c'è una sola chiave disponibile e l'Autorizzato che ne ha bisogno deve chiederla al "Responsabile delle chiavi". Chi accedesse deve annotarlo in apposito registro. Il Dirigente Scolastico, in quanto Titolare, ha libertà assoluta di accesso.

Dati personali comuni - protezione dall'accesso fisico non autorizzato: i documenti contenenti dati personali comuni sono conservati in archivi ad accesso selezionato: pertanto l'accesso ai dati è consentito ai soli Autorizzati del trattamento.

I documenti possono essere estratti dall'archivio e affidati alla custodia dell'Autorizzato del trattamento per il tempo strettamente necessario al trattamento medesimo: egli ha cura di garantirne la riservatezza e provvede al deposito in archivio al termine delle operazioni. Gli Autorizzati che custodiscono dati personali su supporto cartaceo devono verificare che la dotazione di arredi (cassettiere, armadi ecc.) muniti di meccanismi di serratura adatta a garantire la sicurezza sia adeguata, altrimenti devono segnalare al Titolare la necessità di acquisirli.

Dati particolari (sensibili e giudiziari) - protezione dall'accesso fisico non autorizzato: l'accesso è limitato agli Autorizzati del trattamento. Gli archivi devono essere ad accesso controllato, quindi con gestione del registro. Tali documenti devono essere conservati in elementi di arredo (armadi o cassettiere) muniti di serratura a chiave; la chiusura a chiave garantisce tanto la selezione del personale autorizzato ad accedere, quanto il controllo sugli accessi medesimi.

Protezione dei locali archivio contenenti dati personali sensibili:

Se i documenti contenenti dati personali sensibili sono archiviati in arredi (armadi o cassettiere) chiusi a chiave, l'accesso ai locali che li contengono può non essere soggetto a particolari restrizioni. Resta fermo l'obbligo per l'Autorizzato e il Responsabile di verificare che gli elementi di arredo siano sempre chiusi e che vengano rispettate le misure relative alla gestione delle chiavi.

Se non c'è immediata disponibilità di arredi muniti di serratura per l'archiviazione dei documenti contenenti dati personali sensibili, gli archivi devono in ogni caso essere ubicati in appositi locali chiusi a chiave e, se appare agevole l'intrusione dall'esterno, muniti di sbarre. In tal caso il personale diverso dagli Autorizzati del trattamento che vi accede i deve essere accompagnato da uno dei soggetti Autorizzati del trattamento o dal custode delle chiavi che deve verificare che non avvenga un accesso illecito ai dati sensibili ivi contenuti.

Ogni stanza-archivio dev'essere chiusa a chiave quando non presenziata, anche se i documenti sono custoditi in contenitori chiusi a chiave, in quanto aumenta il livello di protezione dei dati stessi.

Protezione dal rischio di perdita dei dati dovuta ad eventi fisici

Un archivio è sottoposto al rischio di svariati tipi di eventi che possono provocare la distruzione o il danneggiamento dei documenti. Per ridurre al minimo questo rischio le principali misure da prendere sono le seguenti:

a) evitare eccessivi carichi d'incendio;
b) utilizzare il più possibile contenitori chiusi;
c) applicare in modo assoluto il divieto di fumo dentro la stanza e nelle adiacenze;
d) non lasciare pertugi di quali possano essere gettati materiali o liquidi;
e) nelle vicinanze devono essere presenti idonei dispositivi antincendio;
f) è auspicabile la presenza di un sensore antincendio, anche autonomo.

Misure logistiche:

Il personale addetto al trattamento di dati personali deve porre in essere le misure necessarie a ridurre al minimo i rischi di: accesso fisico non autorizzato, furto o manomissione dei dati da parte di malintenzionati, distruzione o perdita dei dati dovuta ad eventi fisici, perdita accidentale dei dati.

Chiusura a chiave dei contenitori metallici:

Gli armadi e contenitori che ospitano archivi vanno chiusi a chiave alla fine della giornata lavorativa e le chiavi vanno messe in luogo sicuro indicato dal **DSGA** o dal Custode delle chiavi.

2.14 Procedura di Protezione Dati: archiviazione separata

I documenti contenenti dati particolari (sensibili o giudiziari) vanno di norma chiusi in busta di carta, su cui è riportato nome dell'interessato, tipo di documento, data attuale e la scadenza per la eliminazione (se non conoscibile, mettere una data presunta seguita da un punto interrogativo). Per i documenti contenenti dati particolarmente sensibili, invece del nome sulla busta si deve scrivere un codice, la data attuale e la scadenza per la eliminazione.

La corrispondenza tra codice e nome dell'interessato sarà riportata in un foglio o un quaderno, posto in una busta chiusa gestita dal **DS** o **DSGA**, e posto in luogo sicurissimo e protetto.

La busta viene archiviata in uno degli Armadi cosiddetti "dei Dati Protetti" (permanentemente chiuso a chiave, ad accesso controllato, in una stanza normalmente chiusa a chiave quando non presenziata e, possibilmente, protetta da antifurto.

Al posto del documento così protetto viene messo nel fascicolo un foglio con annotazione generica del tipo di documento, della sua collocazione e della scadenza di distruzione.

2.15 Procedura di Protezione Dati: conservazione di registri e altri documenti utilizzati per anni scolastici precedenti e non più utilizzati

Conservazione: molti documenti e registri sono utilizzati per un intero anno scolastico ma solo in quello. Tra questi, i documenti non più utilizzati negli anni seguenti (salvo ricorsi o richieste di accesso legittime) al termine dell'anno scolastico sono impacchettati a gruppi omogenei e chiusi con carta e scotch; sull'involucro viene riportato il contenuto e la scadenza per l'eliminazione. Vengono conservati in una stanza chiusa a chiave ad accesso selezionato. La durata di archiviazione e, quindi, l'eliminazione degli stessi è indicata **nell'allegato 2 del "Manuale dei flussi documentali" dell'IC di Picerno (PZ).**

5.2.10 Procedura di Protezione Dati: archiviazione nel fascicolo personale

I documenti non archiviati nell'Armadio di Protezione dati, finché l'alunno è iscritto o il dipendente è in servizio, vengono conservati nel fascicolo personale. In particolare alcuni dati si situano in una zona di confine tra dato particolare e dato sensibile (ad es. certificati medici generici privi di diagnosi), data la loro bassa pericolosità vengono mantenuti nel fascicolo personale, ma in una cartella separata, fino a fine anno scolastico, poi eliminati come da **Allegato 2** suindicato. Il fascicolo personale è conservato nel relativo archivio corrente: in cassettiere metalliche chiuse a chiave negli orari non lavorativi e normalmente presidiate da almeno un Autorizzato dei trattamenti (ovvero un dipendente assegnato alla segreteria), in una stanza in cui non sono ammessi di regola estranei e che viene chiusa a chiave al di fuori dell'orario lavorativo.

5.2.11 Procedura di Protezione Dati: archiviazione nell'archivio storico

Quando l'alunno ha cessato la frequenza o il dipendente ha cessato di essere in carico alla scuola, il relativo fascicolo personale viene depurato dei documenti non più necessari, quindi archiviato nel corrispondente archivio storico, collocato in una stanza chiusa a chiave, ad accesso selezionato.

5.2.12 Procedura di Protezione Dati: scarto periodico dei documenti

Vale quanto indicato nell'allegato 2 del "Manuale dei flussi documentali" dell'IC di Picerno (PZ).

5.2.13 Procedura di Protezione Dati: distruzione dei documenti

La distruzione di documenti contenenti dati personali di qualunque livello avverrà con modalità di Protezione Dati per impedire che estranei prendano visione del contenuto o, peggio, se ne impadroniscano. Di queste operazioni si occupano solamente Autorizzati, con la qualifica di Collaboratori Scolastici e Assistenti Amministrativi. Se possibile si utilizza un apparecchio che trincia la carta. Altrimenti si provvede a rendere comunque anonimi mediante tagli e cancellature indelebili i documenti sensibili, giudiziari e particolari ad alto rischio. Per gli altri ci si assicurerà che nessuno possa impadronirsene prima della distruzione (o riciclo o conferimento in discarica) da parte dell'ente a cui si conferiranno.

5.2.14 Procedura di Protezione Dati: appunti, bozze e copie superflue

Anche gli appunti, le bozze, le stampe intermedie, le fotocopie superflue costituiscono elemento di rischio, maggiorato quando trattasi di pratiche comprendenti anche documenti sensibili o giudiziari. Pertanto essi vanno distrutti con la prescritta procedura o, se necessario conservarli, archiviati insieme all'originale del documento sensibile o giudiziario.

5.2.15 Procedura di Protezione Dati: cautele nella fase di fotocopiatura

Quando documenti contenenti dati personali di tipo particolare o ad alto livello di delicatezza devono essere fotocopiati, hanno la precedenza su tutti gli altri e devono essere adottate opportune cautele affinché nessun altro ne possa prendere visione. Tranne impossibilità tecnica, l'operazione di fotocopiatura deve essere effettuata dall'Autorizzato che tratta la pratica. L'Autorizzato deve fare in modo che il documento non venga lasciato in giacenza vicino alla fotocopiatrice né prima né dopo la fotocopiatura. A maggior ragione questo si applica se l'operazione di fotocopiatura avviene in una stanza ad accesso libero. Le fotocopie mal riuscite devono sempre essere trincerate o rese illeggibili.

5.2.16 Procedura di Protezione Dati: la movimentazione da parte di terzi

Quando documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza devono essere movimentati attraverso Collaboratori scolastici autorizzati, anche all'interno della scuola, devono essere collocati in busta chiusa. Anche la spedizione postale o la consegna in altro modo deve essere effettuata esclusivamente da Autorizzati che abbiano ricevuto almeno l'autorizzazione a questo ambito di trattamento e che assicurino massima diligenza nella custodia dei plichi.

5.2.17 Procedura di Protezione Dati: pulizia dei locali contenenti archivi

L'accesso di dipendenti o estranei per la pulizia dei locali contenenti archivi cartacei dev'essere effettuata solo con i contenitori chiusi a chiave. Altrimenti le operazioni, peraltro brevi, devono essere effettuate in presenza di un Autorizzato della segreteria. Se vi sono contenuti dati sensibili sono chiudibili in contenitore, la pulizia deve essere effettuata esclusivamente alla presenza di un Autorizzato del trattamento di tali dati.

5.2.18 Procedura di Protezione Dati: ingresso di persone esterne per manutenzione

L'accesso di dipendenti o estranei per la manutenzione dei locali contenenti archivi cartacei o delle attrezzature in tali stanze contenute, dev'essere effettuata solo con i contenitori chiusi a chiave. Altrimenti le operazioni devono essere effettuate in presenza di un Autorizzato. Se dati sensibili o giudiziari non sono chiudibili in contenitore, l'intervento deve essere effettuato esclusivamente alla presenza di un Autorizzato del trattamento di tali dati.

5.2.19 Procedura di Protezione Dati: ingresso di altre persone in segreteria

Di norma l'ingresso in segreteria, nelle ore lavorative, è riservato a chi vi lavora, al Dirigente e ai suoi collaboratori, ai Collaboratori scolastici che ne hanno motivo. Gli altri dipendenti e gli estranei di norma non possono accedere, salvo che ne facciano richiesta preventiva e ne ottengano l'autorizzazione di volta in volta.
Ciò viene previsto allo scopo di evitare che persone non autorizzate vedano anche involontariamente documenti riservati.

La segreteria deve essere chiusa a chiave quando non è presenziata da chi vi lavora. Possibilmente le pulizie devono essere organizzate in orari in cui vi sia almeno un Assistente Amministrativo presente.

5.3 - Trattamenti con strumenti elettronici – documenti informatici o digitali

Categorie di Autorizzati: Assistenti Amministrativi, DSGA, Collaboratori Scolastici, docenti per quanto di loro pertinenza

5.3.1 Procedura di Protezione Dati: sistema di autorizzazione dell'accesso

Il trattamento di dati personali con strumenti elettronici é consentito esclusivamente agli Autorizzati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Le credenziali di autenticazione sono, generalmente, costituite da un codice per l'identificazione dell'Autorizzato (user-id o username o 'nome utente') fisso e parzialmente riservato (è noto al gestore del sistema, perché deve assegnarlo ed è visibile ai manutentori software), e da una password segretissima variabile associata.

Ad ogni Autorizzato sono assegnate individualmente una o più credenziali per l'autenticazione.
Ogni Autorizzato deve adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale (= password segreta o parola chiave).

La parola chiave, quando é prevista dal sistema di autenticazione, dev'essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Essa non deve contenere riferimenti agevolmente riconducibili all'Autorizzato (nomi o iniziali proprie o di parenti, date di nascita, e simili).

La parola chiave dev'essere modificata da ciascun Autorizzato al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave dev'essere modificata almeno ogni tre mesi.

Costituisce infrazione disciplinare gravissima scrivere una password o una user-id su fogli di carta o quaderni, tento peggio se in vicinanza del computer. È vietato anche tenerla nel cassetto, benché chiuso a chiave.

I profili di autorizzazione, per ciascun Autorizzato o per classi omogenee di Autorizzati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

L'implementazione di questo sistema di autenticazione si fa in questo modo:

Il **DS** o il **DSGA** individuano quali profili di autorizzazione sono necessari per gli Autorizzati che utilizzano il computer. In pratica stabiliscono quali computers può usare ogni Autorizzato, di quali cartelle (directories) ha necessità, quali altre cartelle vanno create, a quali cartelle possono accedere tutti gli Autorizzati e a quali possono accedere solo alcuni e a quali soltanto un singolo Autorizzato, quali devono essere cifrate e con quale tecnica.

L'**AmS**, il **DSGA** o un tecnico dovrà tradurre in pratica queste direttive, costruendo i necessari profili di autorizzazione differenziati per ciascun utilizzatore, al quale sarà consegnata la corrispondente credenziale di autenticazione (più d'una se necessario).

Le credenziali di autenticazione non utilizzate da almeno sei mesi vanno disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Le credenziali vanno disattivate anche in caso di perdita della qualità che consente all'Autorizzato l'accesso ai dati personali.

Gli Autorizzati non devono lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. Per brevi periodi, in ragione di massimo 10 minuti, possono utilizzare una semplice password con salvaschermo.

5.3.2 Procedura di Protezione Dati: salvataggio dei dati (back-up)

Gli Autorizzati sono tenuti a salvare i dati correnti o quelli non su piattaforma gestionale (tipo ARGO o Spaggiari) con frequenza almeno settimanale. Pertanto procederanno al back-up su supporto esterno opportunamente scelto dall'**AmS** cioè con caratteristiche che possano garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

5.3.3 Procedura di Protezione Dati: eventuale cifratura dei file recanti dati idonei a rivelare lo stato di salute e la vita sessuale

Per i dati personali particolari che non siano già protetti dal sistema di rete dell'amministrazione, il file va salvato mediante il sistema di cifratura che viene fornito dal DGSA, scelto dal AmS. Le parti di documento o archivio che riguardano questi dati vanno archiviate, se possibile, in un file separato e specifico, rispetto agli altri dati personali dell'interessato.

Ciò viene fatto allo scopo che gli accessi agli dati dell'interessato non implichino anche la possibilità di vedere anche questi dati particolarmente protetti.

La parola chiave o simile utilizzata per la cifratura dev'essere nota soltanto all'Autorizzato, che la scriverà su un foglio di carta con il nome e la collocazione del file e la password. Tale foglio sarà chiuso in busta sul cui esterno si scriverà il nome e la collocazione del file e quant'altro serve per l'identificazione. La busta sarà affidata al DGSA o al nominato "Custode delle Password" se nominato, che la riporrà in luogo sicurissimo.

5.3.4 Procedura di Protezione Dati - Programmi firewall, dispositivi firewall

Accessi abusivi logici (cioè eseguiti attraverso la logica del software)
I dati devono essere permanentemente protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale (accesso abusivo per via telematica da parte di operatori molto esperti nell'utilizzare la connessione della scuola a internet per introdursi nei computer durante il collegamento e copiare dati o manometterli; alcuni di loro sono definiti "hackers").
Molto utile è l'aggiornamento frequente del Sistema Operativo.

La protezione da "intrusioni logiche" può essere effettuata in due modi:

a) uno a bassa sicurezza, con un apposito programma denominato "Firewall" che intercetta ogni utilizzo delle porte di comunicazione del computer sia in entrata che in uscita e verifica se è autorizzato altrimenti lo blocca e chiede di autorizzare o meno la comunicazione.
b) uno ad elevata sicurezza, mediante un apparecchio denominato "Firewall, che si colloca fisicamente tra il modem e il computer. Esso è un tipo particolare di computer, fornito di un apposito software, che realizza le stesse cose di cui al punto precedente, ma in modo decisamente più efficace e affidabile. Il suo software va aggiornato con regolarità.

5.3.5 Procedura di Protezione Dati - Programmi antivirus - Virus, worms (vermi) e altri programmi maligni

I dati devono essere permanentemente protetti contro virus, worms, e altri programmi informatici che possono causare perdita di dati, malfunzionamenti, danni all'hardware, trasmissione all'esterno di files contenuti nel computer). Tali virus possono infettare il computer tramite l'uso di pen drive o l'accesso a certi siti internet o tramite la posta elettronica (in particolare i cosiddetti "allegati"). La protezione viene effettuata mediante l'utilizzo di un programma antivirus, che sarà acquistato dalla scuola e fornito agli Autorizzati dal **DGSA**. Se necessario, si ricorrerà all'intervento di un tecnico esterno o all'**AmS** per l'installazione e la formazione degli Autorizzati alle tecniche di aggiornamento e di utilizzo. Il programma antivirus deve sempre essere aggiornato. L'Autorizzato è tenuto a verificare che queste condizioni siano attuate e ad eseguire quanto è di sua pertinenza.
Prima di aprire ciascun messaggio di posta elettronica l'Autorizzato è tenuto a valutare se il messaggio proviene da mittente noto o plausibile, in caso contrario deve adottare particolari cautele. Non deve aprire allegati che abbiano estensione ".exe", ".pif", ".scr" a meno che non sia sicuro del mittente; se l'estensione appare doppia (esempio: "pif.scr" non deve aprire comunque l'allegato). Inoltre deve valutare dal titolo dell'allegato se esso è plausibile e pertinente col mittente e con le attività di interesse della scuola.
3.6 Procedura di Protezione Dati: uso dei supporti rimovibili

Le pen drive o hard disk esterni non devono essere utilizzati mai per memorizzare i file contenenti dati personali; tali files vanno invece memorizzati solo nel disco fisso di computers protetti da sistema di credenziali di accesso. Ciò al fine di evitare che chi si impadronisca di tali supporti rimovibili, possa accedere ai dati. I supporti rimovibili devono essere utilizzati esclusivamente per le copie di sicurezza (back-up) e subito devono essere riposti nel luogo sicuro indicato.

5.3.7 Procedura di Protezione Dati: cautele nel riutilizzo dei supporti rimovibili

I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Autorizzati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili (= riformattando il disco e verificando l'avvenuta riformattazione; non basta assolutamente cancellare i files!)

5.3.8 Procedura di Protezione Dati – accesso di manutentori software o hardware

Se una delle misure minime di sicurezza elencate sono attuate tramite l'intervento di soggetti esterni alla propria struttura, per provvedere alla esecuzione è assolutamente tassativo ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni sulla sicurezza informatica Tale dichiarazione va consegnata al titolare.

In caso di manutenzione dell'hardware o del software da parte di persone esterne alla scuola o comunque non incaricate del trattamento dei dati contenuti in quel computer, un Autorizzato deve controllare a vista le operazioni eseguite, in modo da verificare che non ci sia mai lettura o copia di dati né che siano indebitamente scoperte le parole chiave.

5.3.9 Procedura di Protezione Dati: pulizia dei locali

L'accesso di dipendenti o estranei per la pulizia dei locali contenenti dischi di back-up o hard disk esterni dev'essere effettuata solo con i contenitori chiusi a chiave. Se dati sensibili o giudiziari non sono chiudibili in contenitore, la pulizia deve essere effettuata alla presenza di un Autorizzato del trattamento di tali dati. Durante l'accesso per la pulizia tutti i computer contenenti dati sensibili o giudiziari devono essere spenti (o in modalità salvaschermo con password di ripristino) oppure deve presenziare un Autorizzato del trattamento di tali dati.

5.3.10 Procedura di Protezione Dati: ingresso di persone esterne per manutenzione locali o impianti o attrezzature

Stanze contenenti dischi o hard disk di back-up: l'accesso di dipendenti o estranei per la manutenzione dei locali o delle attrezzature in tali stanze contenute, dev'essere effettuata solo con i contenitori chiusi a chiave. Se dati sensibili o giudiziari non sono chiudibili in contenitore, l'intervento deve essere effettuata alla presenza di un Autorizzato del trattamento di tali dati. Durante l'accesso per l'intervento tutti i computer contenenti dati sensibili o giudiziari devono essere spenti oppure deve presenziare un Autorizzato del trattamento di tali dati. Si noti che sottraendo un disco di back-up, un malintenzionato può ricostruire gli archivi della scuola, violando dati personali.

5.3.11 Procedura di Protezione Dati: scelta del software

Nella scelta del software, va esplicitamente verificato se ogni programma è realizzato in modo da attuare le misure di sicurezza informatiche. In particolare che sia consentito l'accesso multiplo basato su credenziali, che gli archivi siano cifrati, che i programmi che trattano sia dati non sensibili che dati sensibili siano in grado di archiviare quest'ultimi a parte e non li renda visibili insieme agli altri dati, ma sia necessario accedere specificamente ad essi, eventualmente con una seconda protezione con credenziali.

5.3.12 Procedura di Protezione Dati: accesso ai dati in assenza dell'Autorizzato o variazione degli autorizzati

Qualora, in caso di assenza dell'Autorizzato assegnatario della dotazione informatica, si renda necessario per ragioni improrogabili l'utilizzo di dati accessibili in via esclusiva con i suoi codici di accesso è necessario rispettare le seguenti regole:

1) deve sussistere un'improrogabile necessità di accedere ai dati per ragioni di servizio;
2) deve essere verificata l'impossibilità o la notevole difficoltà di raggiungere l'Autorizzato;
3) il **DGSA** = ("Custode delle password") apre la busta chiusa riposta in luogo sicuro dov'è scritta la password dell'Autorizzato. Poi la mette in una nuova busta chiusa con la nuova da affidare al sostituto.
4) Al rientro dell'Autorizzato il **DSGA** annulla la password del sostituto e chiede a questi di riporre in un busta chiusa la nuova password per accedere ai servizi informatici di sua competenza.

Il **DSGA** è il "custode delle password e vi può accedere per controlli e verifiche, anche il **DS** può disporre delle password. Per la gestione delle password si utilizza la modulistica allegata (Allegato 1 alla PP3).

5.3.13 Procedura di Protezione Dati: protezione dal furto di computers portatili contenenti dati personali

Chi sottraesse un computer portatile avrebbe la possibilità di accedere ai dati personali eventualmente in esso contenuti. Considerata la facilità con cui possono essere sottratti, tali computer non devono essere utilizzati per dati sensibili o giudiziari. Vanno rigorosamente chiusi in armadio di sicurezza o cassaforte quando non utilizzati.

5.3.13 Procedura di Protezione Dati: invio documenti cartacei o digitalizzati

Nel caso fosse necessario e lecito inviare dati personali particolari a terzi si possono presentare i seguenti casi:

Procedura di Anonimizzazione

Documenti originali cartacei da cui occorre eliminare tutti i dati personali e invio cartaceo: cancellare una copia con penna ad inchiostro e successivamente con pennarello nero tutti i dati personali (non è sufficiente il solo pennarello nero, in trasparenza il dato risulterà ancora leggibile), quindi spedire i documenti.

Documenti originali cartacei da cui occorre eliminare tutti i dati personali e invio in forma digitale via mail: cancellare una copia con penna e successivamente con pennarello nero tutti i dati personali e scannerizzare il documento da inviare via e_mail o su supporto digitale.

Procedura di Pseudonimizzazione

Documenti originali digitali da cui occorre eliminare tutti i dati personali e invio in forma digitale: sostituire ai dati personali (nome, cognome, classe di appartenenza o qualsiasi altro dato che possa identificare l'interessato) un numero o un codice. Il codice deve essere noto solo agli Autorizzati di segreteria al **DSGA** e al **DS.** La corrispondenza codice interessato sarà svelata solo agli autorizzati all'occorrenza su disposizione del **DS** o del **DSGA.**

Procedura di Cifratura

Documenti originali digitali che devono essere trasferiti necessariamente e lecitamente con i dati particolari dell'interessato in modo identificabile e invio in forma digitale: occorre cifrare il documento con un **software di cifratura** affidabile e aggiornato (al momento **tipo RSA**) e inviare il file cifrato via mail possibilmente tipo PEC che garantisce maggiore sicurezza.

6 - Trattamenti da parte dei docenti

Categorie di Autorizzati: Docenti

6.1 Procedura di Protezione Dati: registri

Eventuali registri cartacei devono essere sempre custoditi in modo sicuro, riposti nel cassetto del docente se non utilizzati e mai lasciati alla portata degli alunni o di terzi non autorizzati.

Qualora si utilizzino registri di classe cartacei questi devono essere consultabili solo dagli alunni della classe interessata e si deve vigilare perché non vi siano accessi non autorizzati. I collaboratori scolastici sono Autorizzati di riporli in luogo sicuro al termine delle lezioni.

I registri relativi ai BES o relativa documentazione cartacea (PdP, PEI, ecc) devono essere custoditi dai docenti specializzati, non lasciati in classe. Non devono in alcun modo lasciar intravedere i dati relativi all'allievo/i interessati.

I registri dei verbali, affidati per la scrittura, la firma o la consultazione, devono essere protetti da accessi non autorizzati e riconsegnati quanto prima al Dirigente o alla segreteria per essere riposti in luogo sicuro.

6.2 Procedura di Protezione Dati: certificazioni mediche e informazioni sullo stato di salute degli alunni

I dati personali in grado di rivelare lo stato di salute sono classificati particolari e quindi protetti dalla visione di terzi che non sia strettamente necessaria. Quindi eventuali certificati medici vanno visionati solo se necessario e subito restituiti all'interessato affinché li consegni in Segreteria. Questo vale in particolare per i certificati di esonero o limitazione presentati per educazione fisica; l'insegnante prenda nota dei limiti da osservare e faccia recapitare dall'interessato il certificato in Segreteria. A volte l'insegnante ottiene informazioni su particolari, anche gravi, problemi di salute dell'alunno che possono presentarsi durante le lezioni, in alcuni casi con grave rischio per la vita dell'alunno (allergie con pericolo di grave shock anafilattico, asma grave con pericolo di soffocamento, diabete grave, epilessia, cardiopatie gravi, ecc.) o imbarazzanti (disturbi di continenza, ecc.), messe a disposizione dai genitori o dall'interessato. Se l'informazione è orale l'insegnante è tenuto al riserbo. Se esiste qualche comunicazione scritta, trattasi di dato sensibile e va trattato con particolari cautele, chiedendo al DS o al DSGA come fare.

Anche informazioni su particolari diete seguite dall'alunno o per motivi di salute o per motivi religiosi sono da considerare dato sensibile, pertanto va rivelato soltanto nei casi strettamente necessari ed omettendone la ragione.

I dati relativi ad alunni diversamente abili il cui handicap incide sulla didattica, sono di altissima sensibilità. Pertanto i documenti dovranno essere visionati soltanto dai docenti e dal personale strettamente necessario, conservati con elevata cautela, poi consegnati in Segreteria in busta chiusa su cui sarà annotato nome dell'interessato, descrizione del contenuto, data e l'annotazione "Da conservare separatamente in armadio sicuro". Al loro posto, insieme agli altri elaborati si metterà un foglio con l'annotazione del luogo di conservazione.

6.3 Procedura di Protezione Dati: elaborati contenenti notizie particolari

Nel caso un elaborato consegnato alla scuola contenga dati personali o familiari particolari, va custodito con cura e poi riposto in busta chiusa nell'armadio degli elaborati debitamente chiuso a chiave; sulla busta sarà annotato nome dell'interessato, descrizione del contenuto, data e l'annotazione "Da conservare separatamente in armadio sicuro". Al suo posto, insieme agli altri elaborati si metterà un foglio con l'annotazione del luogo di conservazione. Più semplicemente, piuttosto che estrapolare solo gli elaborati contenenti dati sensibili e conservarli separatamente dagli altri, si conservino tutti gli elaborati della classe in armadio sicuro.

6.4 Procedura di Protezione Dati: gestione degli elenchi degli alunni

Anche gli elenchi contenenti soltanto dati anagrafici degli alunni godono di protezione. Pertanto possono essere consegnati a terzi, soprattutto privati, esclusivamente per attività istituzionali della scuola e previa visione dell'informativa del ricevente. Va comunque previamente chiesta l'autorizzazione al Dirigente perché potrebbe costituire atto illegittimo.

6.5 Procedura di Protezione Dati: gestione di documenti scolastici

In generale qualunque documento scolastico che contenga dati personali di qualcun altro è sottoposto dal RGPD a una qualche forma di protezione, quindi va custodito in modo che nessun altro possa visionarlo, copiarlo o impadronirsene. Se non c'è motivo di detenerlo, va riconsegnato in Segreteria per l'archiviazione.
5 - Trattamenti da parte dei membri di organi collegiali (anche esterni alla scuola)
Categorie di Autorizzati: membri di organi collegiali.
5.1 Procedura di Protezione Dati: gestione di documenti scolastici

In generale qualunque documento scolastico che contenga dati personali di qualcun altro è sottoposto dal RGPD a una qualche forma di protezione, quindi va custodito in modo che nessun altro possa visionarlo, copiarlo o impadronirsene. Se non c'è motivo di detenerlo, va consegnato in segreteria per l'archiviazione.
L'obbligo è ancora più stringente se il dato è di tipo particolare, sensibile o giudiziario.
Chi avesse originale o copia di un tale documento deve custodirlo con cura dalla visione di terzi e riconsegnarlo alla segreteria appena non serve più. È vietato conservarlo quando è cessato il motivo istituzionale per cui il dato è stato acquisito.
Anche gli elenchi contenenti soltanto dati anagrafici degli alunni godono di protezione da parte RGPD. Pertanto possono essere consegnati a terzi, soprattutto privati, esclusivamente per attività istituzionali della scuola e previa visione dell'informativa del ricevente. Va comunque previamente chiesta l'autorizzazione al Dirigente perché potrebbe costituire atto illegittimo.

7 - Trattamenti da parte dei Collaboratori Scolastici e del Personale Ausiliario

Categorie di Autorizzati: Collaboratori Scolastici e Personale Ausiliario.

7.1 Procedura di Protezione Dati: gestione di documenti scolastici

In generale qualunque documento scolastico che contenga dati personali di qualcun altro è sottoposto dal **RGPD** a una qualche forma di protezione, quindi va custodito in modo che nessun altro possa visionarlo, copiarlo o impadronirsene. Se non c'è motivo di detenerlo, va consegnato in segreteria per l'archiviazione.

L'obbligo è ancora più stringente se il dato è di tipo particolare cioè sensibile o giudiziario.

Chi avesse originale o copia di un tale documento deve custodirlo con elevatissima cura e cautela dalla visione di terzi e riconsegnarlo alla segreteria appena non serve più.

Anche gli elenchi contenenti soltanto dati anagrafici degli alunni godono di protezione da parte **RGPD**. Pertanto possono essere consegnati a terzi, soprattutto privati, esclusivamente per attività istituzionali della scuola.

Va comunque previamente chiesta l'autorizzazione al Dirigente perché potrebbe costituire atto illegittimo. Pertanto qualsiasi registro, elaborato, elenco, libretto personale, certificato, e in generale documento scolastico che contiene dati personali di qualcuno va custodito con cautela, impedendo che altri ne prendano visione, lo copino o se ne impadroniscano.

7.2 Procedura di Protezione Dati: trasporto di documenti scolastici

I documenti ricevuti aperti vanno immediatamente consegnati alla segreteria, senza prenderne visione. Se c'è il sospetto che si tratti di certificati medici, certificazioni relativi ai redditi, ecc. si deve offrire all'interessato una busta chiusa affinché ve li inseriscano.

Nel caso di trasporto di documenti alla posta o ad altri destinatari o di ricezione di documenti destinati alla scuola, vanno trattati con cura, protetti da accesso di terzi, mai lasciati incustoditi, consegnati appena possibile alla segreteria o al legittimo destinatario.

Nel caso di documenti da consegnare internamente alla scuola vanno adottate analoghe cautele.

7.3 Procedura di Protezione Dati: custodia

Le stanze contenenti archivi e non presenziate devono essere mantenute chiuse e si deve intervenire immediatamente se un non-Autorizzato vi accede.

Stanze contenenti archivi non posti in contenitori chiusi a chiave e in cui si conservano anche documenti particolari sono ad accesso controllato, il che significa che la chiave è gestita dal **DGSA** o da un suo delegato "Custode delle chiavi". Chi dovesse accedere per manutenzioni o pulizie, deve farlo chiedendone il permesso, limitando al massimo il tempo di permanenza ed evitando di lasciare la stanza incustodita o di farvi accedere altri; inoltre, se ritenuto necessario dal **DGSA** deve presenziare un addetto alla segreteria.

La Presidenza, la segreteria e gli uffici in genere vanno chiusi a chiave quando non presenziati dal relativo personale.

E' fatto divieto assoluto a chiunque non ne abbia ricevuto esplicita autorizzazione di accendere o utilizzare i computer della segreteria o della presidenza o che comunque contengano dati personali. Si deve intervenire immediatamente se una persona non autorizzata tenta di farlo.

Se esterni per motivi di manutenzione devono entrare nelle stanze citate o negli archivi per i quali è prevista la chiusura a chiave, vanno seguiti a vista; se questo è impossibile, vanno invitati a tornare in altro momento, a meno che non sia in atto un'emergenza urgente che richiede il loro intervento.

Fuori dall'orario di apertura della scuola non si deve far entrare nei locali citati alcun estraneo.

8 – L'Amministratore di Sistema

Seppur non obbligatoria la nomina di un Amministratore di Sistema (**AmS**), figura definita dal Provvedimento del Garante del 2008, aggiornato nel 2009, visto l'uso sempre più intensivo della gestione amministrativa e della didattica con strumenti digitali on line, tale figura si rende necessaria. Tale figura deve avere competenze informatiche adeguate a fornire i servizi come di seguito:

- garantire che i dati personali contenuti nei vari archivi informatici siano custoditi e controllati ai fine di ridurre al minimo i rischi di:
  - distruzione, perdita o modifica anche accidentale dei dati stessi;
  - accesso non autorizzato;
  - trattamento non consentito, o non conforme alle finalità della raccolta.

In relazione a tale incarico, **AmS**, ha il compito di sovrintendere alle risorse del sistema informativo dell'istituto e, in particolare, attenendosi alle disposizioni dei Titolare del trattamento e collaborando con il Responsabile della Protezione dei Dati, deve:

- sovrintendere al funzionamento della rete e monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza informatica;
- effettuare o predisporre interventi di manutenzione hardware e software su sistemi operativi e applicativi;

- aggiornare periodicamente, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, i sistemi informatici per tutelare la protezione dei dati da intrusione, cancellazione, distruzione, modifiche non autorizzate, furto, comunicazione e diffusione non autorizzate, con maggior riguardo ai dati particolari ("sensibili") o giudiziari;
- impartire istruzioni organizzative e tecniche per la custodia, l'uso, il riutilizzo o la distruzione dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti;
- consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati;
- predisporre sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte dell'amministratore di sistema stesso, avendo cura che tali registrazioni (access log) abbiano caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste;
- assistere il Titolare e il Referente del trattamento nell'impostazione e gestione operativa del sistema di attribuzione dei codici di accesso agli strumenti informatici e di autorizzazione al trattamento di dati personali;
- assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso in Istituto collaborando con il custode delle password finalizzate all'accesso al sistema informativo e vigilando sulla sua attività;
- predisporre e rendere funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni e impartire a tutti gli incaricati istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno quotidiana;
- adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
- predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale dell'efficacia delle misure di sicurezza adottate in Istituto, comprese le prove di disaster recovery;
- verificare costantemente che l'Istituto abbia adottato le misure adeguate di sicurezza per il trattamento dei dati personali provvedendo in collaborazione con il Responsabile della Protezione dei Dati agli aggiornamenti eventualmente necessari anche per adeguare il sistema ad eventuali nuove norme in materia di sicurezza;
- verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi di elaborazione;
- comunicare tempestivamente ogni violazione, incidente o palese rischio sulla protezione dei dati, al Titolare e/o al Responsabile della protezione dei dati per permettere l'obbligatoria comunicazione "data breach" e i relativi interventi correttivi;
- garantire l'efficace separazione della rete didattica da quella amministrativa.

9 – Il Data Breach (Violazione dei dati personali)

L'Istituto sensibilizza tutti i dipendenti, i genitori e gli alunni a segnalare tempestivamente al DS o ai suoi collaboratori qualsiasi violazione dei dati personali siano venuti a conoscenza o anche segnalazione di potenziali violazioni a seguito di sospetti malfunzionamenti degli strumenti informatici, e_mail sospette, virus, ecc.
La procedura di riferimento per i casi accertati di Data Breach è la **PP02 Procedura di gestione della Violazione del Dati Personali ("Data Breach")**