



---

---

## Il Dirigente scolastico

**Visto** il decreto legislativo 30 giugno 2003, n.196 recante il Codice in materia di protezione di dati personali, e segnatamente gli artt. 33 e ss., nonché l'allegato B del suddetto D.lgs., contenente il Disciplinare tecnico in materia di misure minime di sicurezza;

**Considerato** che la Dott.ssa Stesina Silvana Dirigente Scolastico della Direzione Didattica di Biella II^ Circolo è titolare del trattamento di dati personali ai sensi dell'art.28 del d.lgs. n. 196 del 2003;

**Visto** l'obbligo di prevedere ed applicare le misure minime di sicurezza di cui agli artt. 31 e ss. del D.lgs. n.196 del 2003;

**Visto** il Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione, emanato con Decreto Ministeriale n.305 del 7.12.2006;

### **Adotta il DOCUMENTO PROGRAMMATICO SULLA SICUREZZA in data 29/03/2007**

Il presente documento, elaborato al fine di mettere in atto le misure di sicurezza per tutelare i dati personali oggetto di trattamento, fornisce una individuazione dei criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati a misure di sicurezza e dei criteri per assicurare l'integrità dei dati, da adottare per il trattamento dei dati personali effettuato dal personale della Direzione Didattica di Biella II^ il cui legale rappresentante pro-tempore è il dirigente scolastico. Dott.ssa Stesina Silvana che nel seguito del documento sarà indicato come "titolare". Il presente documento è aggiornato periodicamente ed i termini utilizzati seguono le definizioni riportate all'art.4 del D.lgs 196/2003. Del documento fanno parte integrante le schede allegate al Regolamento del Ministero della Pubblica Istruzione citato nelle premesse.

## **1 Elenco dei trattamenti di dati personali**

### **1.1 Finalità**

Il trattamento dei dati personali è funzionale al raggiungimento delle finalità di istruzione e di formazione in ambito scolastico, professionale e superiore, con particolare riferimento a quelle svolte anche in forma integrata, ed è quindi di rilevante interesse pubblico, ai sensi degli articoli 20 e 21 del D.lgs 196/2003. Per le sue finalità istituzionali, l'Istituzione scolastica tratta dati personali, sia comuni che sensibili o giudiziari, di studenti, genitori, personale dipendente e fornitori.

### **1.2 Luoghi di tenuta e trattamento dei dati:**

I dati su supporto cartaceo sono conservati negli armadi dell'ufficio di segreteria e nella stanza denominata archivio storico.

I dati acquisiti attraverso il protocollo riservato sono conservati nella cassaforte dell'ufficio del dirigente scolastico.

I dati in formato elettronico risiedono nei computer di tutti i servizi amministrativi.

(Nella tabella che segue, relativamente ai dati sensibili e giudiziari, nella descrizione sintetica del trattamento, le finalità e le attività svolte, i tipi di dati trattati e le operazioni eseguite sono indicati in modo sintetico e con riferimento alle schede allegate al Regolamento del Ministero della Pubblica Istruzione citato nelle premesse, con specificazione, per ogni identificativo di trattamento, delle specifiche schede)

**Tabella 1.1 – Elenco dei trattamenti: informazioni essenziali (regola 19.1 del disciplinare tecnico)**

<b><i>Id Trattamento</i></b>	<b><i>Descrizione sintetica del trattamento</i></b>		<b><i>Natura dei dati</i></b>		<b><i>Strutture Di riferimento</i></b>	<b><i>Altre strutture che concorrono</i></b>	<b><i>Descriz.modalità trattamento</i></b>
<b>T1</b>	<b>Gestione Personale Interno</b> Relativamente ai dati sensibili e giudiziari : Scheda n. 1 –Selezione e reclutamento a tempo indeterminato e determinato e gestione del rapporto di lavoro.	<b>Docenti Dirigente ATA</b>	SI	SI	<b>A 1.2</b>	<b>A 1.1 – A 1.4 - A2 – A3 – A4</b>	<b>Cartaceo/ informatizzato</b>
<b>T2</b>	<b>Gestione Personale Esterno</b> Relativamente ai dati sensibili e giudiziari : Scheda n.1- Gestione del rapporto di lavoro dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato.	<b>Collaboratori esterni-Fornitori</b>	SI	SI	<b>A 1.2</b>	<b>A 1.1 A 1.4</b>	<b>Cartaceo/ informatizzato</b>
<b>T3</b>	<b>Gestione Alunni e genitori</b> Relativamente ai dati sensibili e giudiziari : Scheda n. 4 – Attività propedeutiche all’avvio dell’anno scolastico; Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso.	<b>Genitori Alunni</b>	SI	SI	<b>A1.3</b>	<b>A 2 A 4 A 3</b>	<b>Cartaceo/ informatizzato</b>
<b>T4</b>	<b>Gestione Contenzioso e procedimenti disciplinari</b>  Scheda n.2 – Gestione del contenzioso e procedimenti disciplinari	<b>Personale dipendente Fornitori Collaboratori esterni</b>	SI	SI	<b>A 4</b>		<b>Cartaceo/ informatizzato</b>
<b>T5</b>	<b>Gestione Organi Collegiali e Organi isituzionali</b>	<b>Docenti ATA Genitori</b>	SI	SI	<b>A 1.2 A 1.3</b>	<b>A4</b>	<b>Cartaceo/ informatizzato</b>

<b>T6</b>	<b>Gestione Archivio Storico e corrente- Fotoriproduzione documenti</b> Relativamente ai dati sensibili e giudiziari: Tutte le schede allegate al regolamento sul trattamento dei dati sensibili e giudiziari	<b>Alunni, Genitori, Fornitori, Personale, Altre amministrazioni</b>	<b>SI</b>	<b>SI</b>	<b>Tutte le Aree Segreteria Collabor.i scolastici</b>		<b>Cartaceo/ informatizzato</b>
-----------	---	--	-----------	-----------	---	--	---------------------------------

**Tabella 1.2 – Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti (regola 19.1 del disciplinare tecnico)**

<i><b>Id Trattamento</b></i>	<i><b>Applicativo</b></i>	<i><b>Banca Dati</b></i>	<i><b>Ubicazione fisica dei supporti di memorizzazione</b></i>		<i><b>Tipologia dei dispositivi di accesso</b></i>	<i><b>Tipologia di interconnessione</b></i>
			<i><b>Luogo</b></i>	<i><b>Elaboratore</b></i>		
<b>T1</b>	<b>Software gestionale SISSI</b>	<b>Serversissi</b>	<b>Salaserver</b>	<b>PC serversissi</b>	<b>PC</b>	<b>Internet - Intranet</b>
<b>T1</b>	<b>Software gestionale axios</b>	<b>Serversissi</b>				
<b>T1</b>	<b>Suite Microsoft office</b>	<b>Serversissi</b>	<b>Ufficio segreteria</b>	<b>PC personali</b>	<b>PC</b>	<b>Internet - Intranet</b>
<b>T2</b>	<b>Software gestionale SISSI</b>	<b>Serversissi</b>	<b>Salaserver</b>	<b>PC serversissi</b>	<b>PC</b>	<b>Internet - Intranet</b>
<b>T2</b>	<b>Suite Microsoft office</b>	<b>Serversissi</b>	<b>Ufficio segreteria</b>	<b>PC personali</b>	<b>PC</b>	<b>Internet - Intranet</b>
<b>T3</b>	<b>Software gestionale SISSI</b>	<b>Serversissi</b>	<b>Salaserver</b>	<b>PC serversissi</b>	<b>PC</b>	<b>Internet - Intranet</b>
<b>T3</b>	<b>Suite Microsoft office</b>	<b>Serversissi</b>	<b>Ufficio segreteria</b>	<b>PC personali</b>	<b>PC</b>	<b>Internet - Intranet</b>
<b>T4</b>	<b>Suite Microsoft office</b>	<b>PC Dirigente scolastico</b>	<b>Ufficio Dirigente scolastico</b>	<b>PC personale</b>	<b>PC</b>	<b>- Intranet</b>
<b>T5</b>	<b>Software gestionale SISSI</b>	<b>Serversissi</b>	<b>Salaserver</b>	<b>PC serversissi</b>	<b>PC</b>	<b>Internet - Intranet</b>
<b>T5</b>	<b>Suite Microsoft Office</b>	<b>Pc Ufficio Personale</b>	<b>Ufficio Personale</b>	<b>PC personale</b>	<b>PC</b>	<b>Intranet</b>

<b>T1-T2</b>	<b>Software gestionale Unico Inps-Emens</b>	<b>Pc Ufficio Personale</b>	<b>Ufficio Personale</b>	<b>PC personale</b>	<b>PC</b>	<b>Internet</b>
--------------	---	---------------------------------	--------------------------	---------------------	-----------	-----------------

**Tabella 1.3 – Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti cartacei (regola 19.1 del disciplinare tecnico)**

<b><i>Id Trattamento</i></b>	<b><i>Archivio cartaceo</i></b>	<b><i>Ubicazione logistica</i></b>		
			<b><i>Stanza</i></b>	<b><i>Armadio</i></b>
<b>T6</b>	<b>Raccoglitori cartacei</b>	<b>Scaffalatura con raccoglitori specifici e numerati dell'ufficio</b>	<b>Archivio storico- Uffici di competenza</b>	

## **2 Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati**

Le misure indicate nel presente documento sono relative alla sede centrale dell'istituzione scolastica.

Le procedure di trattamento dei dati avvengono nella sola segreteria, considerato che i dati oggetto delle misure indicate nel presente documento sono trattenuti presso i plessi scolastici solo per il tempo necessario a provvedere all'inoltro alla segreteria. I dati sono trattenuti sotto la responsabilità degli incaricati (docenti e responsabile della sede) in cassetto chiuso del quale detengono la chiave.

Il titolare del trattamento ha designato, ai sensi dell'art.29 D.lgs 196/2003, con atto scritto contenente analitiche istruzioni relative ai compiti affidati, il responsabile del trattamento nella persona del DSGA sig.ra Umilio Grazia.

Il responsabile del trattamento ha provveduto, sulla base della lettera di designazione e delle disposizioni dell'art.30, ad individuare gli incaricati del trattamento dei dati personali appartenenti ai profili professionali del personale ATA; ha conferito agli stessi l'incarico con atto scritto contenente puntuali istruzioni relative agli ambiti di trattamento consentiti, corredato da linee guida e con allegate le schede relative al trattamento dei dati sensibili e giudiziari.

Il Responsabile del trattamento ha provveduto altresì a individuare, nominare e incaricare per iscritto un incaricato della gestione e della manutenzione degli strumenti elettronici, un incaricato della custodia delle copie delle credenziali e un incaricato delle copie di sicurezza delle banche dati ai quali sono state fornite puntuali istruzioni relative ai compiti da svolgere. Il titolare ha direttamente provveduto ad individuare e incaricare il personale docente con atto che fornisce le istruzioni necessarie. I singoli incaricati, che hanno rilasciato ricevuta della avvenuta consegna della lettera di incarico, sono stati informati che l'ambito dei trattamenti autorizzati è suscettibile di aggiornamento periodico e che sono tenuti ad attenersi al divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico, anche per il tempo successivo alla sua cessazione, senza limiti temporali.

La comunicazione dei soggetti previsti dal D.lgs 196/2003 è avvenuta attraverso la pubblicazione all'albo della scuola dell'organigramma della scuola e delle responsabilità.

A tutti gli incaricati del trattamento di dati mediante strumento elettronico sono state conferite credenziali di autenticazioni (art.34, comma 1, lett.b) mediante parola chiave, conformi alle caratteristiche indicate nell'allegato B. Agli incaricati sono state fornite puntuali indicazioni per la modifica della parola chiave ogni tre mesi.

## Competenze e responsabilità delle strutture preposte ai trattamenti

L'ufficio di segreteria si trova a Biella in via Coda 37 al secondo piano; appartiene alla struttura dell'ufficio di segreteria il seguente personale:

- Il Dirigente scolastico
- il Direttore dei servizi generali ed amm.vi
- n. 4 Assistenti amm.vi

La struttura dell'Ufficio di segreteria è ripartita in aree di riferimento:

- A.1.2 AREA PERSONALE
- A.1.3 AREA ALUNNI/ GENITORI
- A.1.4 AREA BILANCIO
- A.1.5 AREA PROTOCOLLO
- A. 4 GESTIONE CONTENZIOSO E PROVVEDIMENTI DISCIPLINARI PERSONALE

Il personale docente svolge le proprie attività nei nove plessi dipendenti dalla Direzione Didattica di Biella II<sup>^</sup> e l'area di riferimento di competenza è:

- A. 2

I Collaboratori scolastici svolgono le proprie attività nei nove plessi dipendenti dalla Direzione Didattica di Biella II<sup>^</sup>, uno è in servizio presso l'ufficio di segreteria: L'area di competenza, relativa alle loro mansioni è:

- A. 3

L'AMMINISTRATORE DI SISTEMA si occupa della gestione sicurezza ,Backup e Restore, ed è attribuito ad una Ditta esterna.

**Tabella 2 – Competenze e responsabilità delle strutture preposte ai trattamenti (regola 19.2)**

<i><b>Id Strutturatura</b></i>	<i><b>Struttura</b></i>	<i><b>Trattamenti effettuati</b></i>	<i><b>Descrizione dei compiti e delle responsabilità</b></i>
A1.1	Ufficio segreteria Area Contabile	T1 – T2 – T6	<ul style="list-style-type: none"> <li>• Acquisizione/inserimento/trattamento e gestione dati contabili e anagrafici per retribuzioni, contratti, ricostruzioni, riscatti, computi , Legge 29, cessioni stipendi, disoccupazione.</li> <li>• Dichiarazioni mensili DM10- Emens-DMA-Pensioni-Mod.770-CUD</li> <li>• Rapporti, trasmissioni documenti personale dipendenti a: MEF-USP-USR</li> <li>• Rapporti con il pubblico</li> <li>• Personale esterni: dati personali e contabili, gestione acquisti e preventivi</li> <li>• Archivio corrente e storico</li> <li>• Calcolo competenze correnti/ accessorie</li> <li>• Inserimento e trasmissione dati sistema centrale/SISSI</li> </ul>

<b>A1.2</b>	<b>Ufficio segreteria Area Personale</b>	<b>T1 -T2- T6 -T5</b>	<ul style="list-style-type: none"> <li>• <b>Rapporti con il pubblico</b></li> <li>• <b>Gestione Graduatorie docenti/ata</b></li> <li>• <b>Gestione,registrazione,rilascio documenti relativi a assenze e svolgimento carriera personale dipendente</b></li> <li>• <b>Inserimento e trasmissione dati sistema centrale e SISSI</b></li> <li>• <b>Rilevazione e trasmissione scioperi</b></li> <li>• <b>Elenchi personale per gestione organi collegiali</b></li> <li>• <b>Archivio corrente e storico</b></li> </ul>
<b>A1.3</b>	<b>Ufficio Segreteria Area Alunni / genitori</b>	<b>T3</b>	<ul style="list-style-type: none"> <li>• <b>Rapporti con il pubblico</b></li> <li>• <b>Iscrizioni,trasferimento,infortunati alunni</b></li> <li>• <b>Gestione e trasmissione statistiche</b></li> <li>• <b>Inserimento , gestione,trasmissione alunni sistema centrale e SISSI</b></li> <li>• <b>Elenchi alunni /genitori per gestione organi collegiali</b></li> <li>• <b>Archivio corrente e storico</b></li> </ul>
<b>A1.4</b>	<b>Ufficio DSGA Area Bilancio</b>	<b>T1 -T2-T6</b>	<ul style="list-style-type: none"> <li>• <b>Rapporti con il pubblico</b></li> <li>• <b>Gestione contratti prestazione lavorative collaboratori esterni</b></li> <li>• <b>Acquisti ,preventivi,ordini,determine</b></li> <li>• <b>Gestione registro fornitori/contratti</b></li> <li>• <b>Rapporti con Banca/Enti/Associazioni/Altre Istituzioni/Privati</b></li> <li>• <b>Predisposizione programma annuale</b></li> <li>• <b>Redazione Conto consuntivo</b></li> <li>• <b>Collaborazione alla stesura dei progetti inseriti nel POF in relazione agli stanziamenti del Programma Annuale</b></li> <li>• <b>Liquidazione competenze accessorie e Fondo Istituto</b></li> <li>• <b>Predisposizione calcolo fondo di istituto e verifica relativa copertura finanziaria in relazione alle attività programmate</b></li> <li>• <b>Verifica al 30 giugno di ogni anno dell'attuazione e delle eventuali modifiche al programma annuale</b></li> <li>• <b>Archivio corrente e storico</b></li> <li>• <b>Inserimento e trasmissione dati sistema centrale/SISSI</b></li> </ul>
<b>A1.5</b>	<b>Ufficio Segreteria Protocollo</b>	<b>T1-T2-T3-T4-T5</b>	<ul style="list-style-type: none"> <li>• <b>Registrazione posta in entrata e uscita</b></li> <li>• <b>Fotoriproduzione documenti /ripartizione pratiche in relazione alle area di competenza</b></li> <li>• <b>Archivio corrente e storico</b></li> </ul>
<b>A2.</b>	<b>Docenti</b>	<b>T5-T3</b>	<ul style="list-style-type: none"> <li>• <b>Registri alunni</b></li> <li>• <b>Assenze alunni</b></li> <li>• <b>comunicazioni scuola - famiglia</b></li> </ul>

<b>A3.</b>	<b>Collaboratori scolastici</b>	<b>T6</b>	<ul style="list-style-type: none"> <li>• <b>Comunicazioni interne nei vari plessi</b></li> <li>• <b>Riproduzione mediante fotocopiatura dei documenti e notifica degli stessi</b></li> </ul>
<b>A4</b>	<b>Dirigente Scolastico</b>	<b>T4</b>	<ul style="list-style-type: none"> <li>• <b>Gestione Contenzioso</b></li> <li>• <b>Provvedimenti disciplinari personale dipendente</b></li> </ul>
<b>A5</b>	<b>Amministratore di Sistema</b>	<b>T7</b>	<ul style="list-style-type: none"> <li>• <b>Amministra il Server di sistema Serversissi con il Dbase SISSI</b></li> <li>• <b>Amministra i sistemi operativi dei clients in rete</b></li> <li>• <b>Amministra e configura il router per l'accesso ad internet</b></li> <li>• <b>Predisporre l'automazione del backup dell'archivio SISSI con l'applicativo Axios</b></li> <li>• <b>Installa sui client della rete amministrativa idoneo Antivirus</b></li> <li>• <b>Installa su tutte le macchine idonei programmi antispywere</b></li> <li>• <b>Utilizza l'applicativo SISSI Gestione Sicurezza per la gestione degli accessi e dei profili</b></li> <li>• <b>Verifica Backup e sistema sicurezza</b></li> <li>• <b>Amministrazione utenti</b></li> </ul>

### **3 Analisi dei rischi che incombono sui dati**

La ricognizione e l'analisi dei rischi, che potrebbero comportare una distruzione, sottrazione, perdita, trattamento abusivo dei dati, di origine dolosa, colposa, ovvero meramente fortuita, in grado di recare pregiudizio ai dati personali trattati, è stata riportata nelle tabelle che seguono nelle quali gli eventi sono stati suddivisi in tre categorie:

#### **1) Comportamenti degli operatori.**

Sottrazione di credenziali di autenticazione; carenza di consapevolezza, disattenzione o incuria; comportamenti sleali o fraudolenti; errori materiali.

#### **2) Eventi relativi agli strumenti.**

Danno arrecato da virus informatici o di programmi suscettibili di recare danno; spamming o tecniche di sabotaggio; malfunzionamento, indisponibilità o usura degli strumenti; accessi esterni non autorizzati; intercettazione di informazioni in rete.

#### **3) Eventi relativi al contesto fisico-ambientale.**

Accessi non autorizzati a locali ad accesso ristretto; eventi distruttivi naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc) nonché dolosi, accidentali o dovuti ad incuria; guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc); errori umani nella gestione della sicurezza fisica.

I suddetti rischi sono stati ripartiti in classi di gravità, tenendo conto della concreta possibilità di realizzazione, adottando la seguente scansione:  
**Alta - Bassa - Molto Elevata - Media - Medio-Alta - Medio-Bassa**

La tabella seguente sintetizza i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutandone l'impatto sulla sicurezza. Le possibili conseguenze e stimandone la gravità, ponendoli altresì in correlazione con le misure di sicurezza previste.

**Tabella 3 – Analisi dei rischi (regola 19.3 del disciplinare tecnico)**

	<b><i>Id Rischio</i></b>	<b><i>Rischi</i></b>	<b><i>Si/No</i></b>	<b><i>Descrizione dell'impatto sulla sicurezza (gravità:alta/media/bassa)</i></b>
<b>Comportamento degli operatori</b>	<b>R1</b>	<b>Sottrazione di credenziali di autenticazione.</b>	<b>Si</b>	<b>Alta</b>
	<b>R2</b>	<b>Carenza di consapevolezza, disattenzione o incuria.</b>	<b>Si</b>	<b>Media</b>
	<b>R3</b>	<b>Comportamenti sleali o fraudolenti.</b>	<b>Si</b>	<b>Bassa</b>
	<b>R4</b>	<b>Errore materiale.</b>	<b>Si</b>	<b>Media</b>
<b>Eventi relativi agli strumenti</b>	<b>R5</b>	<b>Azione di <i>virus</i> informatici o di programmi suscettibili di recare danno.</b>	<b>Si</b>	<b>Alta</b>
	<b>R6</b>	<b><i>Spamming</i> o tecniche di sabotaggio.</b>	<b>Si</b>	<b>Alta</b>
	<b>R7</b>	<b>Malfunzionamento, indisponibilità o degrado degli strumenti.</b>	<b>Si</b>	<b>Media</b>
	<b>R8</b>	<b>Accessi esterni non autorizzati.</b>	<b>Si</b>	<b>Media</b>
	<b>R9</b>	<b>Intercettazione di informazioni in rete.</b>	<b>Si</b>	<b>Media</b>
<b>Eventi relativi al contesto</b>	<b>R10</b>	<b>Accessi non autorizzati a locali/reparti ad accesso ristretto.</b>	<b>Si</b>	<b>Bassa</b>
	<b>R11</b>	<b>Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc,) nonché dolosi, accidentali o dovuti ad incuria.</b>	<b>Si</b>	<b>Media</b>
	<b>R12</b>	<b>Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.).</b>	<b>Si</b>	<b>Media</b>
	<b>R13</b>	<b>Errori umani nella gestione della sicurezza fisica.</b>	<b>Si</b>	<b>Media</b>

#### **4 - Misure in essere e da adottare per garantire l'integrità e la disponibilità dei dati, non che la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità**

Contro i rischi d'intrusione i locali della sede centrale, unica sede nella quale sono detenuti dati soggetti a protezione, sono dotati di impianto d'allarme a sensori infrarossi, attivabile mediante digitazione d'un codice consegnato al personale dipendente. E' stata disposta l'attivazione dell'allarme al termine dell'orario di lavoro.

Per garantire la sicurezza delle aree in cui i dati sono trattati elettronicamente, sono state introdotte sui personal computer password di BIOS e password di rete, trimestralmente cambiate.

Le aree contenenti dati in supporto cartaceo (archivio e mobili contenenti documentazione contabili dei dipendenti e degli alunni) sono ubicate in modo tale che ciascun addetto possa rilevare a vista e impedire il tentativo di accesso da parte di persone estranee.

Sono state impartite disposizioni affinché, in assenza del personale, le stanze rimangano chiuse e le chiavi siano custodite dal personale collaboratore scolastico in servizio addetto alla vigilanza che, al termine del servizio, provvederà al deposito delle chiavi nell'apposito contenitore.

L'ubicazione di stampanti ed apparecchio telefax tradizionale non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale.

Di seguito si illustrano le norme applicate per garantire la sicurezza e l'integrità dei dati per:

- *Computer e supporti informatici:* I computer, inclusi i server, risultano tutti sollevati da terra, in modo da evitare eventuali perdite di dati dovuti ad allagamenti; il server è collegato ad un gruppo di continuità che consente di escludere al perdita di dati derivanti da sbalzi di tensione o di interruzione di corrente elettrica. L'integrità dei dati sul server amministrativo è garantita da una procedura di backup; è effettuata normalmente masterizzando su CD ROM ogni lunedì, i backup di tutta la settimana eseguiti sul server. I CD ROM vengono conservati per almeno due mesi nell'apposta cassaforte ignifuga e stagna alle infiltrazioni di acqua. Tutti i server della rete amministrativa vengono protetti da password per impedire al personale non autorizzato l'accesso alla rete amministrativa. Le password sono assegnate e riportate su un apposito foglio conservato nella cassaforte collocata nella stanza del DSGA. L'introduzione di password di BIOS all'accensione dei personal computer, di password dello screen-saver e di password per l'accesso in rete determina un soddisfacente livello di protezione dei dati contenuti nei PC. L'introduzione delle password e di apposito software antivirus inibisce ad estranei l'uso dei personal computer, attraverso i quali, tramite Proxy, si accede alla posta elettronica.
- Per l'invio di messaggi e-mail a più destinatari, sono state fornite al personale istruzioni affinché quale destinatario venga sempre indicata la scuola con l'indirizzo e-mail e in CCN i destinatari, in modo che non possano essere individuati gli indirizzi e-mail degli altri destinatari attraverso la funzione di proprietà.  
I CD ROM masterizzati contenenti copie degli archivi eseguiti localmente dai computer sono custoditi negli appositi contenitori di plastica e inseriti nella cassaforte sempre chiusa con combinazione alfanumerica su serratura elettronica. I floppy disk contenenti dati degli studenti, delle famiglie degli stessi, dei lavoratori dipendenti e collaboratori, possono essere riutilizzati esclusivamente dopo opportuna formattazione, in modo da impedire la lettura dei dati precedenti, così come stabilito dalla legge. I CD ROM non più utilizzabili vengono distrutti.  
I floppy disk contenenti dati, prima della formattazione, sono custoditi nello stesso modo dei DVD contenenti copie degli archivi. Per quanto riguarda infine l'obbligo previsto dalle misure minime sulla sicurezza di cui all'allegato B del codice della privacy, i computer sono dotati di programma antivirus che è aggiornato sotto la responsabilità del titolare del trattamento a cadenza almeno trimestrale e che consente di rilevare immediatamente all'apertura di un file la presenza di un virus.
- *Supporti cartacei:* relativamente ai supporti cartacei sono state impartite dettagliate istruzioni a tutto il personale al momento dell'affidamento dell'incarico e nel corso degli interventi di formazione. (vedi lettere di individuazione degli incaricati del trattamento dei dati e Linee Guida allegate)

Si rimanda [all'informativa sui diritti dell'utente](#) che accede al sito web della scuola, pubblicato sul sito: [www.Biella](http://www.Biella) II^ e allegato al presente DPS.

Tabella 4.1 – Le misure di sicurezza adottate o da adottare (regola 19.4 del disciplinare tecnico)

<b><i>Id Misura</i></b>	<b><i>Misura</i></b>	<b><i>Descrizione e dei rischi contrastati</i></b>	<b><i>Trattamenti interessati</i></b>	<b><i>Misura già in essere</i></b>	<b><i>Misura da adottare</i></b>	<b><i>Struttura o persone addette all'adozione</i></b>
<b>M1</b>	<b>Predisposizione dei profili di autorizzazione di accesso agli applicativi SISSI</b>	<b>R1,R2,R3, R4</b>	<b>T1-T2-T3-T4</b>	<b>X</b>		<b>A5 – Amministratore di Sistema</b>
<b>M2</b>	<b>Procedura formale di concessione delle credenziali per l'utilizzo degli applicativi SISSI</b>	<b>R1,R2,R3, R4</b>	<b>T1-T2-T3-T4</b>	<b>X</b>		<b>A5 – Amministratore di Sistema</b>
<b>M3</b>	<b>Procedura per la concessione di credenziali per l'accesso all'area riservata di Istruzione.it-SIMPI – posta elettronica-rilevazione scioperi-anagrafe prestazioni-sito Entratel-accesso al servizio di invio conguaglio fiscale-</b>	<b>R1,R2,R3, R T1-T2- T3-T44</b>	<b>T1-T2-T3-T4</b>	<b>X</b>		<b>A1.4 – Ufficio DSGA</b>
<b>M4</b>	<b>Concessione delle credenziali per l'accesso ai dispositivi di amministrazione del sistema informativo</b>	<b>R1,R2,R3, R4, R8,R9</b>	<b>T1-T2-T3-T4</b>	<b>X</b>		<b>A5 – Amministratore di Sistema</b>
<b>M5</b>	<b>Concessione delle credenziali per l'accesso di ciascun utente del sistema alle risorse de dominio -installazione Antivirus sui PC della rete Amministrativa -redazione di procedure organizzative per la verifica della procedura di ripristino e la conservazione dei supporti di memorizzazione removibili -Predisposizione di un piano di interventi di manutenzione dell'Hardware al fine di garantire l'integrità dei dati</b>	<b>R1,R2,R3, R4</b>	<b>T1-T2-T3-T4</b>	<b>X</b>		<b>A5 – Amministratore di Sistema</b>
<b>M6</b>	<b>Procedura di concessione delle autorizzazioni all'accesso dei documenti cartacei</b>	<b>R10,R13</b>	<b>T1-T2-T3-T4</b>	<b>X</b>		<b>A1.4 – Ufficio DSGA</b>
<b>M7</b>	<b>Installazione nei locali in cui sono contenuti gli archivi informatici e cartacei di un impianto antifurto</b>	<b>R10,R13</b>	<b>T1-T2-T3-T4</b>	<b>X</b>		<b>A4 – Dirigente scolastico</b>

<b>M8</b>	<b>Predisposizione di armadi provvisti di chiusura per la custodia dei documenti</b>	<b>R10,R13</b>	<b>T1-T2-T3-T4</b>	<b>X</b>		<b>A4 – Dirigente scolastico</b>
<b>M9</b>	<b>Procedura formale di consegna delle chiavi degli armadi agli incaricati dei trattamenti</b>	<b>R10,R13</b>	<b>T1-T2-T3-T4</b>	<b>X</b>		<b>A3.2 – Ufficio DSGA</b>
<b>M10</b>	<b>Procedura formale di concessione delle autorizzazioni per l'accesso ai locali</b>	<b>R10,R13</b>	<b>T1-T2-T3-T4</b>	<b>X</b>		<b>A3.2 – Ufficio DSGA</b>

**Tabella 4.2 – Scheda descrittiva delle misure adottate**

<b>Scheda n°1</b>		<b>Compilata da DSGA</b>		<b>Data di compilazione</b>	14 dicembre 2005
<b>Misura</b>	<b>M1</b>				
<b>Descrizione sintetica</b>	<b>Predisposizione dei profili di autorizzazione di accesso agli applicativi SISSI</b>				
<b>Elementi Descrittivi</b>	Tramite il programma di gestione sicurezza di SISSI SOFTWARE, assegnazione all'utente identificato dal DSGA di nome utente e password per l'accesso al software specifico di lavoro. L'accesso al software SICUREZZA SISSI è consentito all'amministratore di sistema.				
<b>Data di aggiornamento</b>	15 marzo 2007				

**Tabella 4.2 – Scheda descrittiva delle misure adottate**

<b>Scheda n°2</b>		<b>Compilata da DSGA</b>		<b>Data di compilazione (Modifica)</b>	14 dicembre 2005
<b>Misura</b>	<b>M2</b>				
<b>Descrizione sintetica</b>	<b>Procedura formale di concessione delle credenziali per l'utilizzo degli applicativi SISSI</b>				
<b>Elementi Descrittivi</b>	Comunicazione da parte del DSGA del nome dell'utente e dell'applicativo che andrà ad utilizzare. Scelta della password usata per l'accesso. La password viene comunicata all'utente in busta chiusa con il nome utente utilizzato per l'accesso. L'elenco completo delle password è custodito in apposita cassaforte accessibile tramite codice di accesso.				
<b>Data di aggiornamento</b>	15 marzo 2007				

**Tabella 4.2 – Scheda descrittiva delle misure adottate**

<b>Scheda n°3</b>		<b>Compilata da DSGA</b>		<b>Data di compilazione (Modifica)</b>	14 dicembre 2005
<b>Misura</b>	<b>M3</b>				
<b>Descrizione sintetica</b>	<b>Procedura per la concessione di credenziali per l'accesso all'area riservata di Istruzione.it-SIMPI – posta elettronica-rilevazione scioperi-anagrafe prestazioni-sito Entratel-accesso al servizio di invio conguaglio fiscale-</b>				
<b>Elementi Descrittivi</b>	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				
<b>Data di aggiornamento</b>	15 marzo 2007				

**Tabella 4.2 – Scheda descrittiva delle misure adottate**

<b>Scheda n°12</b>		<b>Compilata da DSGA</b>		<b>Data di compilazione</b>	14 dicembre 2005
<b>Misura</b>	<b>M4</b>				
<b>Descrizione sintetica</b>	<b>Concessione delle credenziali per l'accesso ai dispositivi di amministrazione del sistema informativo</b>				
<b>Elementi Descrittivi</b>	Il Dirigente scolastico e il DSGA individuano un soggetto esterno, in possesso delle relative competenze informatiche, che amministra il sistema.				
<b>Data di aggiornamento</b>	15 marzo 2007				

**Tabella 4.2 – Scheda descrittiva delle misure adottate**

<b>Scheda n°13</b>		<b>Compilata da DSGA</b>		<b>Data di compilazione (Modifica)</b>	14 dicembre 2005
<b>Misura</b>	<b>M5</b>				
<b>Descrizione sintetica</b>	<b>Concessione delle credenziali per l'accesso di ciascun utente del sistema alle risorse de dominio</b>				
<b>Elementi Descrittivi</b>	E' stato creato un profilo comune di rete generico. Le credenziali concesse sono tali da non recare nessun tipo di accesso deleterio per i dati archiviati.				
<b>Data di aggiornamento</b>	15 marzo 2007				

**Tabella 4.2 – Scheda descrittiva delle misure adottate**

<b>Scheda n°14</b>		<b>Compilata da DSGA</b>		<b>Data di compilazione (Modifica)</b>	14 dicembre 2005
<b>Misura</b>	<b>M5</b>				
<b>Descrizione sintetica</b>	<b>Installazione Antivirus sui PC della rete Amministrativa</b>				
<b>Elementi Descrittivi</b>	Il software antivirus è installato singolarmente sia sul server che sui clients. L'aggiornamento del l'antivirus viene effettuato in automatico via internet.				
<b>Data di aggiornamento</b>	15 marzo 2007				

**Tabella 4.2 – Scheda descrittiva delle misure adottate**

<b>Scheda n°15</b>		<b>Compilata da DSGA</b>		<b>Data di compilazione (Modifica)</b>	14 dicembre 2005
<b>Misura</b>	<b>M5</b>				
<b>Descrizione sintetica</b>	<b>Redazione di un disciplinare tecnico per le procedure di Backup con cadenza almeno settimanale -redazione di procedure organizzative per la verifica della procedura di ripristino e la conservazione dei supporti di memorizzazione removibili</b>				
<b>Elementi Descrittivi</b>	. La cadenza del bck è giornaliera, un' ulteriore copia del bck viene effettuata ogni sette giorni su supporto magnetico dvd/cd che viene conservato per due mesi nella apposita cassaforte ignifuga in dotazione. Dei salvataggi viene registrata la data di effettuazione. Ogni settimana, con un programma gestionale BACKUP e RESTORE viene simulato un ripristino del database su un computer di supporto.				
<b>Data di aggiornamento</b>	15 marzo 2007				

**Tabella 4.2 – Scheda descrittiva delle misure adottate**

<b>Scheda n°17</b>		<b>Compilata da DSGA</b>		<b>Data di compilazione (Modifica)</b>	14 dicembre 2005
<b>Misura</b>	<b>M5</b>				
<b>Descrizione sintetica</b>	<b>Configurazione o ripristino del sistema operativo dei clients</b>				
<b>Elementi Descrittivi</b>	Ogni clients è fornito all'origine di disco di ripristino del sistema operativo. In caso di danneggiamento del sistema l'Amministratore di sistema, individuato e incaricato con apposito provvedimento reinstalla e riconfigura le funzionalità dell'apparecchio.				
<b>Data di aggiornamento</b>	15 marzo 2007				

**Tabella 4.2 – Scheda descrittiva delle misure adottate**

<b>Scheda n°18</b>		<b>Compilata da DSGA</b>		<b>Data di compilazione (Modifica)</b>	14 dicembre 2005
<b>Misura</b>	<b>M5</b>				
<b>Descrizione sintetica</b>	<b>Predisposizione di un piano di interventi di manutenzione dell'Hardware al fine di garantire l'integrità dei dati</b>				
<b>Elementi Descrittivi</b>	La verifica del funzionamento hardware è fatta con cadenza annuale. Le verifiche vengono effettuate sul server di rete SISSI. Sul server SISSI è installato il data base generale dei dati sia didattici che sensibili. La verifica principale consiste nel testare l'efficienza dei lettori cd-rom e l'integrità del Hard-disk.				
<b>Data di aggiornamento</b>	15 marzo 2007				

**Tabella 4.2 – Scheda descrittiva delle misure adottate**

<b>Scheda n°19</b>		<b>Compilata da DSGA</b>		<b>Data di compilazione (Modifica)</b>	14 dicembre 2005
<b>Misura</b>	<b>M6</b>				
<b>Descrizione sintetica</b>	<b>Procedura di concessione delle autorizzazioni all'accesso dei documenti cartacei</b>				
<b>Elementi Descrittivi</b>	Il DSGA individua, in base ai compiti assegnati ad ogni assistente amministrativo, la concessione ad accedere ai relativi archivi cartacei.				
<b>Data di aggiornamento</b>	15 marzo 2007				

**Tabella 4.2 – Scheda descrittiva delle misure adottate**

<b>Scheda n°20</b>		<b>Compilata da DSGA</b>		<b>Data di compilazione (Modifica)</b>	14 dicembre 2005
<b>Misura</b>	<b>M 7</b>				
<b>Descrizione sintetica</b>	<b>Predisposizione di armadi provvisti di chiusura per la custodia dei documenti</b>				
<b>Elementi Descrittivi</b>	Ogni Assistente Amministrativo assegnato all'ufficio preposto e tenuto alla conservazione dei documenti negli appositi armadi provvisti di serratura con chiave.				
<b>Data di aggiornamento</b>	15 marzo 2007				

**5 Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento**

Al fine di garantire il ripristino dei dati in seguito a distruzione o danneggiamento, l'istituzione scolastica dispone di idonee procedure di salvataggio periodico (backup) che consistono nell'utilizzo dell'apposito software di backup del programma di gestione amministrativo il quale crea in automatico una copia compressa dei dati, archiviandoli in un'apposita cartella del server, e di un masterizzatore DVD che salva i dati anche su disco DVD registrabile, da utilizzarsi giornalmente al termine dell'orario lavorativo.

**Tabella 5.1 – Criteri e procedure per il ripristino della disponibilità dei dati (regola 19.5 del disciplinare tecnico)**

<b>Ripristino</b>		
<b>Banca dati / archivio dati</b>	<b>Criteri e procedure per il salvataggio e il ripristino dei dati</b>	<b>Pianificazione delle prove di ripristino</b>
<b>Documenti di Office application</b>	<b>E' stata predisposta una attività pianificata sul pc dell'utente di una masterizzazione della cartella documenti</b>	<b>Quindicinale</b>
<b>Documenti Posta elettronica</b>	<b>E' stata predisposta una attività pianificata sul PC utilizzato per la posta elettronica di masterizzazione dei dati di posta</b>	<b>Quindicinale</b>

**Tabella 5.2 – Criteri e procedure per il salvataggio dei dati (regola 19.5 del disciplinare tecnico)**

<i>Salvataggio</i>			
<i>Banca dati</i>	<i>Criteri e procedure per il salvataggio</i>	<i>Luogo di custodia delle copie</i>	<i>Struttura o persona incaricata del salvataggio</i>
<b>Supporto Magnetico DVD</b>	<b>Copia archivi su DVD registrabile</b>	<b>Cassaforte Ignifuga e a tenuta stagna</b>	<b>Amministratore di Sistema</b>

## **6 Previsione di interventi formativi degli incaricati del trattamento**

Gli interventi formativi sono programmati nell'ambito del piano di formazione e aggiornamento del personale, con cadenza annuale, per rendere gli incaricati del trattamento edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. Sono previste idonee attività di formazione in occasione di innovazioni e/o modifiche delle norme e in relazione allo sviluppo scientifico/tecnologico dei mezzi e dei sistemi di protezione.

La formazione è altresì programmata al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali. L'incarico al trattamento dei dati contiene, oltre alle istruzioni date dal responsabile, anche le linee guida per il trattamento dei dati, le informazioni relative al significato dei termini e le schede allegate al Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione. Gli incaricati partecipano alla riunione annuale per la verifica e la revisione del documento programmatico per la sicurezza. Verrà valutata l'eventuale partecipazione del personale della scuola alle iniziative formative organizzate dall'USR del Lazio.

**Tabella 6 – Pianificazione degli interventi formativi previsti (regola 19.6 del disciplinare tecnico)**

<i>Descrizione sintetica degli interventi formativi</i>	<i>Classi di incarico o tipologie di incaricati interessati</i>	<i>Tempi previsti</i>
Attuazione delle norme sulla riservatezza dei dati personali – Acquisizione di competenze giuridiche e di organizzazione scolastica – Responsabilità dei docenti nel trattamento dei dati personali con riferimento al REGOLAMENTO sul trattamento dei dati sensibili e giudiziari	Docenti incaricati del trattamento dei dati personali	1 ore di attività di formazione in un incontro di 1 ora – a.s. 2006/07
Miglioramento dell'attuazione delle norme sulla riservatezza dei dati personali nella scuola	Personale ATA della scuola	2 ore di attività di formazione– a.s. 2006/07

## **7 Descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare**

Dati personali sono gestiti dal sistema informativo del MPI che non ha ancora comunicato le misure adottate e alcun documento programmatico.

## **8 Individuazione dei criteri da adottare per la cifratura o per la separazione dei dati personali idonei a rivelare lo stato di salute e la vita sessuale (Regola 19.8 del disciplinare tecnico)**

Pur non rientrando fra gli organismi tenuti alla attuazione del punto 24, l'istituzione scolastica ha messo in atto particolari misure di protezione nell'archiviazione dei dati personali idonei a rivelare lo stato di salute, conservandoli sempre in busta chiusa inserita all'interno del fascicolo personale.

## **9 Conclusioni**

Il presente documento sarà tempestivamente aggiornato nel caso di sostituzione di attrezzature o di cambiamenti nella disposizione degli spazi di lavoro e, in ogni caso, entro il 31 marzo di ciascun anno.

Agli incaricati del trattamento è stata data informazione circa il contenuto del presente documento, attraverso la consegna di una copia, con rilascio di ricevuta dell'avvenuta consegna, nella quale si dà atto della comunicazione dell'obbligo di uniformarsi al documento.

Il responsabile del trattamento è tenuto a vigilare sull'osservanza delle disposizioni stesse da parte degli incaricati e a emanare ulteriori disposizioni relative alla gestione della sicurezza dei dati.

Il presente documento è stato illustrato nel corso di apposite riunioni, tenute in orario di lavoro, alle quali hanno partecipato il Dirigente Scolastico, il responsabile del trattamento ed il personale ATA incaricato del trattamento, nel rispetto delle disposizioni del D.Lgs 196/03 che prevede l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

In occasione delle riunioni, che saranno successivamente previste per la formazione, si provvederà anche alla valutazione ed alla revisione delle misure di sicurezza.

Le attività di formazione del personale incaricato e di revisione del presente documento vengono annotate in apposito registro verbale tenuto dal Responsabile del trattamento.

Il presente documento verrà illustrato ai docenti nella riunione del Collegio dei Docenti del 29/03/2007, con particolare riferimento a quanto attiene alle documentazioni ed ai dati personali che vengono consegnati agli stessi e alle istruzioni date ai docenti incaricati del trattamento dei dati.

Data 15 marzo 2007

Il titolare del trattamento  
IL DIRIGENTE SCOLASTICO  
**Silvana Stesina**