

ISTITUTO COMPRENSIVO G. LA PIRA  
SAN DONNINO – CAMPI BISENZIO (FI)

IL DIRIGENTE SCOLASTICO

Visto il decreto legislativo n.196 del 30 giugno 2003, riguardante il Codice in materia di trattamento e protezione di dati personali;

Visto l'allegato B del suddetto d.lgs. (da art. 33 a art. 36) contenente il Disciplinare tecnico in materia di misure minime di sicurezza;

Considerato che l'Istituto con sede in Piazza Costituzione Campi Bisenzio, nella persona del suo rappresentante legale Prof.ssa SOMIGLI Stefania, ai sensi dell'art.28 del d.lgs. n. 196/2003 è titolare del trattamento di dati personali e quindi tenuta a definire ed attuare le misure minime di sicurezza di cui agli artt. 31 e ss. Dello stesso d.lgs.;

Visto che l'Istituto, per l'espletamento della sua funzione, didattica e formativa, raccoglie e tratta dati personali dei soggetti coinvolti nell'esercizio di questa funzione, anche con l'intervento di soggetti esterni;

**ADOPTA il seguente  
DOCUMENTO PROGRAMMATICO DELLA SICUREZZA**

**1.0 CONTENUTO DEL DPS**

Il DPS contiene i seguenti elementi espressamente previsti al punto 19 dell'Allegato B del D. Lgs. 196 del 30/06/2003.:

1. Elenco dei trattamenti di dati personali;
2. Elenco dei dati personali di natura comune, sensibile o giudiziaria
3. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
4. Analisi dei rischi incombenti sui dati;
5. Misure adottate per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
6. Criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
7. Programma degli interventi formativi degli incaricati del trattamento;
8. Criteri previsti per garantire il rispetto delle misure minime per i trattamenti di dati personali affidati all'esterno della struttura;
9. Trattamenti di dati personali sensibili o giudiziari con strumenti elettronici affidati all'esterno.

Il DPS quindi definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali presso l'Istituto e riguarda il trattamento di tutti i dati personali – comuni, giudiziari e sensibili elaborati con strumenti elettronici o/e altri strumenti di elaborazione ad esempio cartacei, audio, visivi e audiovisivi, ecc.

**1.1 ELENCO DEI TRATTAMENTI DI DATI PERSONALI.**

Al fine di perseguire l'attività istituzionale primaria di erogazione di servizi formativi, l'istituto tratta dati personali (sia comuni che sensibili o giudiziari) di studenti, personale dipendente, fornitori. I trattamenti sono effettuati, anche per le seguenti finalità correlate: adempimento agli obblighi di fonte legislativa, nazionale o comunitaria, regolamentare o derivante da atti amministrativi; gestione e formazione del personale; adempimenti assicurativi; tenuta della contabilità; gestione delle attività informative curate ai sensi della legge 7 giugno 2000, n.150 contenente la "disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni"; attività strumentali alle precedenti.

I dati trattati sono conservati su supporti informatici e/o cartacei e sono noti all'istituto, in ragione di :  
atti e/o dichiarazioni provenienti da soggetti interessati a fruire direttamente, o a beneficio dei minori sottoposti alla potestà ex art.316 c.c., dei servizi formativi;  
documenti contabili connessi alla fornitura di prestazioni e/o di servizi e/o di lavori;  
documentazione bancaria, finanziaria e/o assicurativa;  
documenti inerenti al rapporto di lavoro, finalizzati anche agli adempimenti retributivi e/o previdenziali.

## **1. 2 ELENCO DEI DATI PERSONALI DI NATURA COMUNE O SENSIBILE.**

Sulla base delle precisazioni di cui sopra , l'istituto, in prima ricognizione, con la previsione di procedere all'aggiornamento del DPS entro il 31.3.2006 come previsto dalla normativa in vigore, dichiara, con riferimento ai destinatari o familiari dei destinatari dell'offerta formativa ovvero del personale coinvolto, a qualunque titolo, nella medesima, o interessato ad essere coinvolto, ovvero di soggetti, a qualsiasi titolo, coinvolti in rapporti negoziali con l'istituto, o aspiranti ad assumere tale ruolo, di trattare i dati di seguito elencati:

- a) Dati identificativi, ai sensi dell'art.4, comma 1, lettere b) e c) del d.lgs. n.196 del 2003, univocamente riconducibili ad un soggetto fisico, identificato o identificabile, quali nominativo, dati di nascita, residenza, domicilio, stato di famiglia, codice fiscale, stato relativo all'adempimento degli obblighi di leva.
- b) Dati identificativi, ai sensi dell'art.4, comma 1, lettere b) e c) del d.lgs. n.196 del 2003, univocamente riconducibili a persone giuridiche, enti o associazioni, inerenti la forma giuridica, la data di costituzione, la sede, il domicilio, l'evoluzione degli organi rappresentativi e legali, la sede, la Partita IVA, il Codice fiscale, la titolarità di diritti o la disponibilità di beni strumentali;
- c) Dati sensibili, ai sensi dell'art.4, comma 1, lett.d) del d.lgs. n.196 del 2003;
- d) Dati giudiziari, ai sensi dell'art.4, comma 1, lett.e) del d.lgs. n.196 del 2003;
- e) Dati inerenti il livello di istruzione e culturale nonché relativi all'esito di scrutini, esami, piani educativi individualizzati differenziati;
- f) Dati inerenti le condizioni economiche e l'adempimento degli obblighi tributari;
- g) Dati riferibili a procedimenti giudiziari, pendenti in qualsiasi grado, o pregressi, di natura civile, amministrativa, tributaria, presso autorità giurisdizionali italiane o estere, diversi da quelli rientranti nell'art.4 comma 1, lett.e) del d.lgs. n.196 del 2003;
- h) Dati atti a rilevare la presenza presso l'istituzione scolastica dei destinatari dell'offerta formativa ovvero dei familiari nonché del personale coinvolto, a qualsiasi titolo, nella somministrazione di tale offerta;

- i) Dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;
- k) Dati inerenti negoziazioni e relative modalità di pagamento rispetto a forniture di beni, servizi o di opere, ovvero proposte ed offerte inerenti le medesime negoziazioni;
- l) Dati inerenti la fornitura e le modalità di pagamento riguardo ad attività professionale a fini formativi;
- m) Dati contabili e fiscali;
- n) Dati inerenti la titolarità di diritti, il possesso o la detenzione di beni mobili registrati, mobili o immobili;
- o) Dati detenuti in applicazione di disposizioni di origine nazionale o comunitaria, atti o provvedimenti amministrativi, fonti contrattuali.

### **1.3. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI.**

Il Dirigente Scolastico titolare del trattamento dei dati personali ha designato, mediante il proprio decreto di nomina (allegato al presente DPS) quale Responsabile ai sensi dell'art.29 del d.lgs. n.196 del 2003 Il Direttore S.G.A. dell'Istituto Kingsley Franks nato a Nigeria il 22/02/1951, preposto alle funzioni di Responsabile del trattamento dei dati personali, in considerazione della esperienza, capacità ed affidabilità espressa dal medesimo, tale da offrire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento.

Il suddetto Responsabile del trattamento ha ricevuto adeguate istruzioni riguardo:

- a) l'individuazione ed adozione delle misure di sicurezza da applicare nell'ambito dell'istituzione scolastica, al fine di salvaguardare la riservatezza, l'integrità, la completezza e la disponibilità dei dati trattati;
- b) l'esigenza di provvedere, mediante atto scritto, all'individuazione delle unità legittimate al trattamento, per mezzo dei singoli preposti, ovvero di singoli incaricati, ai sensi dell'art.30 del d.lgs. n.196 del 2003, deputati ad operare sotto la diretta autorità del responsabile, attenendosi alle istruzioni impartite, fermo restando l'obbligo gravante sul responsabile, di vigilare sul rispetto delle misure di sicurezza adottate.
- c) l'esigenza di verificare che gli obblighi di informativa siano stati assolti correttamente, ovvero che sia stato conseguito il consenso degli interessati;
- d) l'obbligo di collaborare con il titolare nell'adempiere alle richieste avanzate dal Garante per la protezione dei dati personali ovvero alle autorità investite dei poteri di controllo;
- e) l'attribuzione della competenza ad elaborare e sottoscrivere notificazioni al Garante per la protezione dei dati personali;
- f) l'obbligo di osservare e far osservare il divieto di comunicazione e diffusione dei dati personali comunque trattati da parte dell'istituzione scolastica;
- g) l'obbligo di proporre soluzioni organizzative che consentano un ampliamento dei livelli di sicurezza

#### **1.3.1 COMPITI E RESPONSABILITÀ DEL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI**

Il titolare del trattamento dei dati personali ha la responsabilità e l'obbligo di:

- assicurare l'adozione delle misure di sicurezza ai sensi del CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA dei dati stessi;
- nominare il Responsabile della sicurezza dei dati;
- di informativa nei confronti dell'interessato.

### **1.3.2. IL RESPONSABILE DELLA SICUREZZA DEI DATI**

Il responsabile della sicurezza dei dati nominato dal dirigente scolastico è il Direttore dei servizi generali ed Amm.vi Kingsley Franks che accetta la nomina. Nella lettera di nomina il Dirigente Scolastico ha informato il Direttore S.G.A. in merito alle responsabilità a lui affidate in relazione a quanto disposto dalla normativa in vigore ed ha ricevuto dallo stesso Dirigente Scolastico una copia della normativa..

#### **1.3.2.1 Compiti e funzione del Responsabile della sicurezza dei dati personali**

Il Direttore S.G.A. in qualità del responsabile della sicurezza dei dati personali

- garantisce che tutte le misure di sicurezza riguardanti i dati personali siano applicate da tutti gli incaricati;
- redige e aggiorna l'elenco delle sedi in cui vengono trattati i dati;
- redige e aggiorna l'elenco degli uffici in cui vengono trattati i dati;
- nel caso di trattamento con i mezzi informatici, redige e aggiorna l'elenco dei sistemi di elaborazione;
- nomina per ciascun ufficio in cui viene effettuato il trattamento dei dati, un incaricato con il compito di controllare i sistemi, le apparecchiature e l'accesso negli uffici;
- definisce e verifica periodicamente le modalità di accesso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini di loro custodia e accessibilità;
- nel caso di trattamento con i mezzi informatici:
  - a) redige e aggiorna l'elenco dei sistemi di elaborazione;
  - b) assicura che le credenziali di autenticazione non potranno essere assegnate ad altri incaricati, neppure in tempi diversi;
  - c) assicura che le credenziali di autenticazione non utilizzate da almeno sei mesi siano disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica
  - d) assicura che le credenziali di autenticazione siano disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali;
  - e) assicura che il trattamento dei dati personali sia consentito solamente agli incaricati dotati di credenziali di autenticazione con le caratteristiche previste dalla normativa

#### **1.3.2.2 DECLINAZIONE DI RESPONSABILITA'**

Il trattamento dei dati avviene attraverso modalità diverse: strumenti elettronici, interni (P.C.) ovvero collegati in rete fra loro, e/o mediante collegamenti alla rete intranet ed alla RUPA, e/o alla rete internet. Con riferimento alla gestione dei dati mediante rete ministeriale e RUPA, l'Istituto declina ogni responsabilità, operando come semplice utente,

non essendo in grado di intervenire sulla gestione delle informazioni ivi contenute e gestite.

### 1. 3.3 Altre funzioni assunte dal Direttore S.G.A.

Per assicurare maggior coordinamento delle attività dell'istituto in materia di sicurezza dei dati, Il Direttore S.G.A ha assunto anche le seguenti funzioni:

- a) la funzione del responsabile della gestione e della manutenzione degli strumenti informatici;
- b) la funzione dell' Incaricato della custodia delle copie delle credenziali;
- c) la funzione del responsabile di uno specifico trattamento dei dati personali

#### 1. 3.3.1. Compiti e funzione del Responsabile della gestione e della manutenzione degli strumenti informatici

- attivazione delle credenziali di autenticazione a tutti gli incaricati del trattamento dei dati personali effettuati con strumenti elettronici;
- definizione delle politiche per la protezione del sistema contro i virus informatici e verifica dell'efficacia con cadenza semestrale;
- protezione degli elaboratori dal rischio di intrusione;
- attuazione delle misure di rimedi nell'eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

#### 1.3.3.2. Compiti e funzione dell'incaricato alla custodia delle copie delle credenziali

- Custodia delle credenziali per l'accesso ai dati degli incaricati del trattamento;
- Predisposizione per ogni incaricato del trattamento di una busta sulla quale è indicato il nome dell'incaricato e all'interno della busta la credenziale usata;
- Conservazione delle buste con le credenziali in luogo chiuso è protetto;
- Accertamento che tutti gli incaricati siano istruiti sull'uso delle parole chiave, sulle caratteristiche che devono avere e sulle modalità per la loro modifica in autonomia;
- Revoca delle credenziali non utilizzate in caso di perdita della qualità che consentiva all'incaricato l'accesso ai dati personali o nel caso di mancato utilizzo per oltre sei mesi;
- Custodia delle credenziali per l'accesso ai dati degli incaricati del trattamento;
- Per eventuale accesso straordinario l'incaricato della custodia delle copie delle credenziali ha il compito di assicurare la disponibilità dei dati e degli strumenti informatici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile intervenire per necessità di operatività e di sicurezza dei sistemi. L'incaricato della custodia delle copie delle credenziali deve informare tempestivamente l'incaricato del trattamento ogni qualvolta sia stato effettuato un tale tipo di intervento.

#### 1.3.3.3 Compiti del responsabile di uno specifico trattamento dei dati personali

- nomina gli incaricati del trattamento per le banche di dati che gli sono state affidate;
- sorveglianza che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice in materia di dati personali;
- dà le istruzioni adeguate agli incaricati del trattamento effettuato con strumenti elettronici e non;

- verifica periodicamente la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati del trattamento dei dati personali.

#### 1.3.4. Incaricato delle copie di sicurezza delle banche dati

Il Direttore S.G.A ha affidato al Sig. Mastrandrea Franco l'incarico dell'effettuazione delle copie di sicurezza delle banche dati. La lettera di nomina è stata controfirmata per accettazione dal nominato dopo aver preso conoscenza dei compiti e responsabilità connesse alla nomina.

Il Direttore S.G.A in qualità del Responsabile della sicurezza dei dati personali ha provveduto a consegnare al Sig. Mastrandrea Franco quale incaricato dell'effettuazione delle copie di sicurezza delle banche dati una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

##### 1.3.4.1 Compiti e funzione dell'incaricato delle copie di sicurezza delle banche dati

- effettuare periodicamente le copie di sicurezza delle banche dati gestite secondo i criteri stabiliti dal Responsabile della sicurezza dei dati personali (Il Direttore S.G.A.).
- assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro e ad accesso controllato;
- segnalare tempestivamente al Responsabile della gestione e della manutenzione degli strumenti elettronici ogni eventuale problema dovesse verificarsi nella normale attività di copie delle banche dati

#### 1.3.5. INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

Il Responsabile del trattamento, ai sensi dell'art. 30 del D.Lgs. n.196 del 2003, ha provveduto ad individuare gli incaricati autorizzandoli al trattamento dei dati in possesso dell'istituto esclusivamente con riferimento all'espletamento delle funzioni ad essi assegnate.

Gli incaricati sono istruiti in merito alla circostanza che:

- a) il trattamento e la conservazione dei dati deve avvenire in modo lecito e proporzionato alle funzioni istituzionali e nel rispetto della riservatezza;
- b) la raccolta, registrazione ed elaborazione dei dati, mediante strumento informatico o cartaceo, deve essere limitata alle finalità istituzionali;
- c) è loro responsabilità la correzione od aggiornamento dei dati posseduti, l'esame della loro pertinenza rispetto alle funzioni
- d) è loro responsabilità l'inosservanza delle istruzioni riguardanti la comunicazione, effettuata in qualsiasi maniera, dei dati in possesso ai soggetti diversi dagli interessati agli stessi dati, ovvero soggetti non legittimati a ricevere dette comunicazioni.

Tutti gli incaricati sono nominati mediante atti allegati al presente DPS dal Direttore S.G.A. Tali atti (le lettere di nomina) sono debitamente controfirmati per accettazione e specificano i compiti e le responsabilità relative agli incarichi che gli sono affidati in relazione a quanto disposto dalle normative in vigore e riguardanti la sicurezza del trattamento dei dati. Tutti gli incaricati hanno ricevuto dal Direttore S.G.A. una copia della normativa in vigore in materia di sicurezza dei dati personali.

A tutti gli incaricati, destinati al 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  
(Il Disciplinare tecnico in materia di misure minime di sicurezza)

Gli incaricati del trattamento dei dati personali presso l'istituto sono:

- 1) Romani Barbara – Ufficio Protocollo
- 2) Vollandri Patrizia – Ufficio Patrimonio
- 3) Mastrandrea Franco – Ufficio amministrazione e elaborazione dati
- 4) Gabriella Quaia – Ufficio alunni
- 5) Mazza Luigi – Ufficio alunni
- 6) Fiorella – Ufficio alunni
- 7) Forciniti Giovanni – Ufficio personale docente Infanzia/Primaria
- 8) Campana Elisabetta – Ufficio personale docente Media
- 9) Caccavale Paola – Ufficio personale ATA
- 10) Docenti – gestione registri di classe e registro personale dell'insegnante

#### 1.3.5.1 Compiti e responsabilità degli incaricati del trattamento dei dati personali

- Conservazione con la massima segretezza delle parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- La parola chiave deve essere composta da almeno otto caratteri;
- La parola chiave deve essere modificata almeno ogni sei mesi;
- In caso di trattamento di dati sensibili e/o giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- Gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti debbono essere controllati e custoditi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
- Separazione degli atti e documenti contenenti dati sensibili e/o giudiziari da quelli contenenti solo dati comuni.

Per meglio precisare la ripartizione delle funzioni di cui sopra, ambito dei trattamenti, natura dei dati trattati e gli strumenti in uso, si rinvia alla seguente tabella:

**Tabella 1 Strutture preposte ai trattamenti e riparto delle responsabilità**

STRUTTURA	RESPONSABILE	INCARICATO	TRATTAMENTI E COMPITI DELLA STRUTTURA	NATURA DEI DATI TRATTATI	STRUMENTI IN UTILIZZO
Ufficio Protocollo	Kingsley Franks)	Romani Barbara	<p>Protocollo della corrispondenza in arrivo e in partenza</p> <p>Circolari interne: distribuzione e invio ai plessi</p> <p>Smistamento della corrispondenza fra i vari uffici e relative copie come indicato dalla D.S. e dal D.S.G.A.</p> <p>Archiviazione degli atti e conseguente servizio di archiviazione anche degli anni passati</p> <p>Uso posta elettronica</p> <p>gestione contributi volontari genitori</p> <p>attività collaterale con i revisori dei conti rapporto con la Banca e gestione C/C postale</p> <p>Trattamenti strumentali alle attività degli organi collegiali: convocazione, raccolta delle delibere; sistemazione verbali .</p> <p>Attività per Il Patentino</p>	Dati sensibili e comuni	Personal computer e server interno collegati in rete locale e Internet

Ufficio personale	Kingsley Franks)	Paola Caccavale	<p>Gestione del personale di ruolo e non di ruolo ATA</p> <p>Controllo dell'orario di servizio di tutto il personale tramite cartoline marcatempo e registri presenza</p> <p>Tenuta registro degli orari con annotazioni individuali delle ore da recuperare a credito o a debito del dipendente. Invio riepilogo mensile al dipendente</p> <p>Organici</p> <p>Tenuta fascicoli del personale non riservato</p> <p>Tenuta registro perpetuo del personale e altri registri obbligatori</p> <p>Gestione delle assenze: congedi, aspettative e assenze varie e registrazione relativi decreti.</p> <p>Registrazione negli appositi registri, comunicazione alla R.P.S. e alla D.P.T. per eventuali riduzioni di stipendio.</p> <p>Altri adempimenti relativi alle assenze su sissi e simp- Contratti del pers.le ATA a T.D. supplenti temporanei</p> <p>Periodi di prova del personale</p> <p>- Ferie del personale</p> <p>Statistiche relative al personale area di gestione</p> <p>Pratiche di piccoli prestiti e cessione del 5° dello stipendio</p> <p>Quote aggiunte di famiglia, detrazione d'imposta, modalità di riscossione ed ogni altra pratica relativa allo stipendio</p> <p>Certificati di servizio, attestati, dichiarazioni e nomine per attività del personale ATA</p> <p>Gestione delle graduatorie personale non di ruolo: valutazione e punteggio</p> <p>Graduatoria interna pers.le ATA usi</p> <p>Richiesta visite fiscali su criteri del DS.</p> <p>Infortuni al personale</p> <p>Modello 11</p> <p>Richiesta documenti di rito del personale a t.i. e a t.d.</p> <p>Lettera di eventuale incarico al personale gestito Dichiarazione dei servizi arretrati personale ATA</p> <p>Registrazione mensa gratuita docenti e gestione assegni circolari</p> <p>Attività connesse all'applicazione della legge sulla sicurezza dei dati e privacy</p>	Dati sensibili e comuni	Personal computer e server interno collegati in rete locale e Internet
-------------------	------------------	-----------------	--	-------------------------	--

Ufficio personale	Kingsley Franks	Elisabetta Campana	<p>Gestione del personale di ruolo e non di ruolo docenti scuola media Organici</p> <p>Tenuta fascicoli del personale non riservato</p> <p>Registro perpetuo del personale</p> <p>Gestione delle assenze, registrazione negli appositi registri, comunicazione alla R.P.S. e alla D.P.T. per eventuali riduzioni di stipendio.</p> <p>Contratti del personale a T.D. supplenti temporanei</p> <p>Periodi di prova del personale</p> <p>Ferie del personale</p> <p>Statistiche relative al personale</p> <p>Pratiche di piccoli prestiti e cessione del 5° dello stipendio</p> <p>Quote aggiunte di famiglia, detrazione d'imposta, modalità di riscossione ed ogni altra pratica relativa allo stipendio</p> <p>Certificati di servizio, attestati, dichiarazioni</p> <p>Gestione delle graduatorie personale non di ruolo: valutazione e punteggio</p> <p>Registrazione degli atti relativi alle assenze e servizi al Sissi</p> <p>Adempimenti con il Simpi</p> <p>Collegio dei docenti: elenchi del personale</p> <p>Provvedimenti consequenziali alle assenze</p> <p>Richiesta visite fiscali su criteri del DS.</p> <p>Graduatorie interne per eventuali perdenti posto o altri scopi</p> <p>Infortuni al personale</p> <p>Modello 11</p> <p>Richiesta documenti di rito del personale a t.i. e a t.d.</p> <p>Dichiarazione dei servizi arretrati docenti Sc. Media; Funzionario vigilanza anti fumo; Attività connesse all'applicazione della legge sulla sicurezza dei dati e privacy .</p> <p>Figure sensibili antincendio.</p>	Dati sensibili e Comuni	Personal computer e server interno collegati in rete locale e Internet
-------------------	-----------------	--------------------	--	-------------------------	--

Ufficio personale	Kingsley Franks	Forciniti Giovanni	<p>Sostituzione del personale assente di ruolo e non di ruolo di scuola materna e elementare. Organici. Tenuta fascicolo del personale con richiesta di documenti di rito per il personale a TD e a TI. Registri obbligatori del personale Controllo registri firme docenti Elem. e materne Periodi di prova del personale. Richiesta visite fiscali su criteri del DS. Gestione assenze: congedi, aspettative ecc; decreti e registrazione decreti Registrazione degli atti relativi alle assenze e altri servizi al sissi e simpi Ferie del personale. Statistiche relative al personale gestito Certificati di servizio e attestati Lettera di incarico al personale gestito. Graduatorie del pers.le non di ruolo e graduatorie interne pers.le di ruolo. Impegni docenti presso altre scuole (segnalazione alla dirigenza) Trasferimenti – assegnazioni provvisorie/utilizzazioni Segnalazione ore eccedenti per la sostituzione dei docenti e nomine di sostituzione. Attività gestione supplenze; Corsi di aggiornamento del personale Commissione di collaudo Attività connesse all'applicazione della legge sulla sicurezza dei dati e privacy Figure sensibili – antincendio</p>	Dati sensibili e comuni	Personal computer e server interno collegati in rete locale e Internet
-------------------	-----------------	--------------------	--	-------------------------	--

<p>Ufficio amministrativo e elaborazione dati</p>	<p>Kingsley Franks</p>	<p>Mastrandrea Franco</p>	<p>Retribuzioni fisse e accessorie a carico del bilancio dell'Istituto.  Mod. TFR supplenti temporanei e annuali  Dichiarazioni INPS per disoccupazione e requisiti ridotti e normali  Conguagli fiscali/contributivo  Ricostruzione di carriera personale di ruolo e religione  Inquadramento  Elaborazione CUD  Dichiarazione dei redditi – mod.770  Dichiarazione Irap  Posta elettronica  Trasferimenti e passaggio di ruolo: istruttoria pratica e valutazione del punteggio.  Apertura partita di spesa fissa del personale a T.I. e a T.D. nominati fino al termine delle lezioni o fino al 31/8.  compenso retribuito per ferie non godute e decreti relativi.  Adempimenti vari su SIMPI  Attività /pratiche connesse al decentramento amm.vo (autonomia) e previdenza complementare  Prestazioni aggiuntive:  Intensificazione di lavoro per:  Dich. dei servizi docenti Sc. Elem/materna  Aggiornamento Sissi su server e nelle postazioni  Attività connesse all'applicazione della legge sulla privacy  Trasmissione telematica DM/10/tfr</p>	<p>Dati sensibili e comuni</p>	<p>Personal computer e server interno collegati in rete locale e Internet</p>
---	------------------------	---------------------------	--	--------------------------------	---

Ufficio alunni	Kingsley Franks	Cecchi Fiorella	<p>Trattamenti strumentali alla predisposizione e concreta erogazione dell'offerta formativa (raccolta delle domande di iscrizione; condizioni sanitarie ed economiche dei destinatari dell'offerta formativa, documentazione concernente opzioni per insegnamenti facoltativi, dati inerenti profili sanitari o relativi al nucleo familiare dei destinatari dell'offerta formativa, per il riconoscimento di attività di sostegno in ragione di situazioni di disagio, sociale, economico o familiare, registri relativi alle presenze presso l'istituzione scolastica)</p> <p>Area Alunni:  Viaggi d'Istruzione: rapporto con gli alunni, docenti, consigli di classi e dirigente scolastico  Mensa scolastica e trasporto alunni.  Iniziative didattiche: prenotazioni, trasporto visite guidate, compilazione modulistica.  Infortuni alunni: denunce e tenuta registro.  Libri di testo: adozioni, conferme, pubblicazione.  Elezioni di carattere annuale e triennale ed elenchi dei genitori per votazioni</p> <p>Area Patrimonio:</p> <p>Tenuta e aggiornamento registro  Inventario generale  Tenute e aggiornamento registro di facile consumo  Rapporto con sub – consegnatari  Rapporto con le ditte private per riparazioni varie e il Comune  Copiatrice/preparazione corrispondenze Dirigente scolastico e Direttore S.G.A  Adempimenti vari su SIMPI  Intensificazione lavoro per:  segreteria alunni e amm.va  settore affari generali  Attività progetti d'Istituto: fase verifica e variazione  Rapporti con il Comune per la gestione dei beni , mensa, trasporto e pre-scuola  Attività connesse all'applicazione della legge sulla sicurezza dei dati.</p>	Dati sensibili e comuni	Personal computer e server interno collegati in rete locale e Internet
-------------------	--------------------	--------------------	---	-------------------------------	--

Ufficio alunni	Kingsley Franks	Mazza Luigi	<p>Trattamenti strumentali alla predisposizione e concreta erogazione dell'offerta formativa (raccolta delle domande di iscrizione; condizioni sanitarie ed economiche dei destinatari dell'offerta formativa, documentazione concernente opzioni per insegnamenti facoltativi, dati inerenti profili sanitari o relativi al nucleo familiare dei destinatari dell'offerta formativa, per il riconoscimento di attività di sostegno in ragione di situazioni di disagio, sociale, economico o familiare, registri relativi alle presenze presso l'istituzione scolastica)</p> <p>Tenuta del Registro generale degli alunni. Iscrizioni, controllo frequenza, trasferimenti, nulla-osta, foglio notizie alunni, rapporti scuola-famiglia. Statistiche varie. Tenuta e conservazione fascicoli alunni. Gestione alunni h. certificazione, riunioni PEP. Insegnamento religione cattolica e relativi esoneri. Ingressi anticipati e posticipati, ritardi. Diplomi e attestati. Schede di valutazione. Tenuta registro Diplomi. Registrazione assenze e segnalazione dei casi particolari alla dirigenza Scrutini e Esame di Licenza Gestione delle riunioni degli organi collegiali . Adempimenti vari su SIMPI Intensificazione di lavoro per: La gestione area alunni (statistica e monitoraggio) anche per i progetti d'Istituto Rapporto con il Comune per monitoraggio riparazioni varie – sede e succursali Pratiche per la sicurezza e applicazione D.L. 626 – sede e succursali Attività connesse all'applicazione della legge sulla sicurezza dei dati.</p>	Dati sensibili e comuni	Personal computer e server interno collegati in rete locale e Internet
-------------------	--------------------	----------------	---	-------------------------------	--

Ufficio Alunni	Kingsley Franks	Quaia Gabriella	<p>Trattamenti strumentali alla predisposizione e concreta erogazione dell'offerta formativa (raccolta delle domande di iscrizione; condizioni sanitarie ed economiche dei destinatari dell'offerta formativa, documentazione concernente opzioni per insegnamenti facoltativi, dati inerenti profili sanitari o relativi al nucleo familiare dei destinatari dell'offerta formativa, per il riconoscimento di attività di sostegno in ragione di situazioni di disagio, sociale, economico o familiare, registri relativi alle presenze presso l'istituzione scolastica)</p> <p>Tenuta del Registro generale degli alunni.</p> <p>Iscrizioni, controllo frequenza, trasferimenti, nulla-osta, foglio notizie alunni, rapporti scuola -famiglia.</p> <p>Tenuta e conservazione fascicoli alunni.</p> <p>Gestione alunni h. certificazione, riunioni PEP.</p> <p>Insegnamento religione cattolica e relativi esoneri.</p> <p>Ingressi anticipati e posticipati, ritardi.</p> <p>Diplomi e attestati. Schede di valutazione. Tenuta registro Diplomi.</p> <p>Registrazione assenze su relativo registro e segnalazione dei casi particolari alla dirigenza.</p> <p>Scrutini e esame di Licenza</p> <p>Gestione riunioni OO CC</p> <p>Adempimenti vari su Simpi</p> <p>Coordinamento delle attività della segreteria alunni e rapporto con la dirigenza per attività didattiche</p> <p>Gestione della Statistica e monitoraggio anche per i progetti</p> <p>Gestione rapporto con alunni stranieri e loro famiglie</p> <p>Graduatoria alunni 1^ sez. scuola materna</p> <p>Attività connesse all'applicazione della legge sulla sicurezza dei dati e privacy</p> <p>Rapporto con il Comune per mensa, trasporti e pre-scuola</p> <p>Organizzazione corsi estivi Lingua Italiana</p> <p>Figure sensibili antincendio.</p>	Dati sensibili e comuni	Personal computer e server interno collegati in rete locale e Internet
----------------	-----------------	-----------------	---	-------------------------	--

Ufficio Patrimoni o e documentazione	Kingsley Franks	Volandri Patrizia	Servizio di biblioteca della sede e dei plessi dell'istituto Collaborazione con gli insegnanti per catalogazione, Attività di prestiti e gestione informatizzata della biblioteca.  Viaggi d'istruzione: rapporto con le agenzie e attività di rendicontazione collaborazione con DSGA per acquisti, determinazione dirigenziali e altri adempimenti connessi con gli acquisti in generale Attività connesse all'applicazione della legge sulla sicurezza dei dati e privacy Documenti e schede per la sicurezza delle macchine e dei materiali di pulizia (L. 626)	Dati sensibili e comuni	Personal computer e server interno collegati in rete locale e Internet
--------------------------------------	-----------------	-------------------	---	-------------------------	--

#### 1.4. ANALISI DEI RISCHI INCOMBENTI SUI DATI.

L'Istituto tramite il responsabile della gestione e della manutenzione degli strumenti informatici avvalendosi di tecnici esterni ha verificato la situazione dei P.C., delle apparecchiature periferiche e le linee di collegamento in rete installati per il trattamento dei dati con lo scopo di controllare l'affidabilità del sistema e dove ha riscontrato la necessità, tenendo conto anche dell'evoluzione della tecnologia informatica per quanto riguarda la sicurezza dei dati trattati, il rischio di distruzione o perdita e il rischio di accesso non autorizzato o non consentito ha provveduto alla loro sostituzione. Ha proceduto quindi ad una ricognizione 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.

Le fonti di rischio individuate sono :

##### 1)Comportamenti degli incaricati e altre persone

Sottrazione di credenziali di autenticazione; imperizia, imprudenza o negligenza degli incaricati al trattamento dei dati; Comportamenti dolosi degli stessi e altre persone estranee all'Istituto; errori materiali;

Accessi non autorizzati negli strumenti informatici mediante uso abusivo di credenziali di autenticazione;

Furto o danneggiamento degli strumenti informatici di trattamento dei dati da persone estranee all'istituto in orario diverso da quello di lavoro. Intercettazione dei dati in occasione di trasmissione in rete;

Errori umani nell'attivazione degli strumenti di protezione.

## 2) Eventi relativi agli strumenti.

Danno arrecato da virus informatici e/o da hackers, spamming o tecniche di sabotaggio;  
Mal funzionamento degli strumenti.

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

Perdita di dati in conseguenza di eventi incontrollabili (terremoto) ovvero, eventi astrattamente preventivabili (incendi o allagamenti) di origine fortuita, dolosa o colposa;  
Guasti a sistemi complementari, come una mancata erogazione di energia elettrica per lunghi periodi di tempo, tale da pregiudicare la climatizzazione dei locali.

I rischi individuati sono classificati sulla base del livello di gravità stimato dall'Istituto, tenendo conto della concreta possibilità di una loro realizzazione, sulla base del seguente sistema di classificazione:

**A = alto MA = medio - alto B = basso MB = medio - basso M = medio**

La seguente tabella sintetizza le principali fonti di rischi per la sicurezza dei dati, le possibili conseguenze, il livello di gravità e le misure di sicurezza previste.

**Tabella 2 Analisi dei rischi**

EVENTO		IMPATTO SULLA SICUREZZA DEI DATI		RIF. MISURE DI AZIONE	
		DESCRIZIONE	GRAVITÀ STIMATA	MISURE ADDOTTE	REVISIONE DELLE MISURE
COMPOR- TAMEN- TI DEGLI OPERATORI	Furto di credenziali di autenticazione	Accessi non autorizzati	<b>MB</b>	Vigilanza sul rispetto delle istruzioni impartite su l'uso delle password. Le password sono custoditi in un luogo sicuro	Come previsto dalla normativa per i codici di autenticazione

	Imperizia, imprudenza, negligenza o incuria e errore materiale degli incaricati	Dispersione, perdita e/o alterazione anche irreversibile dei dati e/o di programmi. Introduzione di dati errati nelle banche dati	<b>B</b>	Formazione e/aggiornamento continuo su programmi e nuove procedure. Vigilanza sul rispetto delle procedure esistenti. Verifica dei dati e la congruenza fra i dati	All'introduzione di nuove procedure e ingresso di nuovi incaricati.
	Comportamenti sleali o fraudolenti degli incaricati	accessi non autorizzati ai dati e l'uso improprio degli stessi.	<b>MB</b>	Uso delle password di accesso nelle aree di trattamento degli incaricati Separazione dei dati sensibili da quelli comuni	Come previsto dalla normativa per i codici di autenticazione.
<b>EVENTI RELATIVI AGLI STRUMENTI</b>	Azione di virus informatici	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori;	<b>MA</b>	Adozione di idonei dispositivi di protezione (Anti virus)	Continua

	Spamming o altre tecniche di sabotaggio	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	<b>MA</b>	Adozione di idonei dispositivi di protezione (dispositivi da individuare)	Continua
	Mal funzionamento, degli strumenti	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	<b>B</b>	Assistenza e manutenzione continua degli elaboratori e dei programmi; ricambio periodico ; rapporto annuale dei rischi sui software	Verifica continua dello stato di funzionamento degli strumenti ; verifica annuale dei sistemi operativi e di software tenendo conto in particolare di disponibilità di nuove versioni migliorative dei software in uso; segnalazioni di patch, fix o system-pack per la rimozione di errori o malfunzionamento e per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamenti dei dati.

	Accessi esterni non autorizzati	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	<b>MB</b>	Adozione di idonei dispositivi di protezione	Revisione dei codici di accesso in seguito alla mobilità del personale oltre che revisione ordinaria prevista dalla normativa in vigore
	Intercettazione di informazioni in rete	Disponibilità dei dati alle persone non autorizzate.	<b>MA</b>	Adozione di idonei dispositivi di protezione (dispositivi da individuare)	
<b>EVENTI RELATIVI AL CONTESTO</b>	Accessi non autorizzati a locali/reparti ad accesso ristretto durante e fuori dall'orario di servizio	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; accesso e uso non autorizzato dei dati; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	<b>M</b> (fuori dall'orario di servizio) <b>B</b> (durante l'orario di servizio)	Protezione dei locali mediante serratura con distribuzione e delle chiavi ai soli autorizzati; Presenza di allarme centrale	Controllo su funzionamento dell'allarme; verifica del rispetto delle istruzioni impartite sulla disponibilità e l'uso delle chiavi

	Asportazione e furto di strumenti contenenti dati	Dispersione e perdita di dati, di programmi e di elaboratori;	<b>MB</b>	Protezione dei locali e dei siti di ubicazione degli elaboratori e dei supporti di memorizzazione mediante serratura con distribuzione e delle chiavi ai soli autorizzati; Presenza di allarme centrale	Controllo su funzionamento dell'allarme; verifica del rispetto delle istruzioni impartite sulla disponibilità e l'uso delle chiavi
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di dati, dei programmi e degli elaboratori	<b>B</b>	Attività di prevenzione, controllo, assistenza e manutenzione periodica, vigilanza sul rispetto delle istruzioni impartite, formazione; copie di sicurezza di programmi e dati e flusso continuo di informazioni e sulla possibilità di eventi distruttivi naturali	Gestione copie di sicurezza di dati e programmi con cadenza giornaliera/settimanale

	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, etc.)	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	<b>B</b>	Attività di controllo, assistenza e manutenzione periodica degli impianti; Copie di sicurezza di programmi e dati
--	---	---	----------	---

#### **1.5. MISURE ADOTTATE PER LA PROTEZIONE DELLE AREE E DEI LOCALI, RILEVANTI AI FINI DELLA LORO CUSTODIA E ACCESSIBILITÀ.**

##### **Misure generali**

In considerazione di quanto disposto dal Codice in materia di dati personali e dal Disciplinare Tecnico in materia di misure minime di sicurezza, viene fatto divieto a chiunque di:

- effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Responsabile della sicurezza dei dati personali di dati oggetto di trattamento;
- effettuare copie fotostatiche non autorizzate dal Responsabile della sicurezza dei dati oggetto di trattamento;
- Sottrarre, cancellare o distruggere senza l'autorizzazione del Responsabile della sicurezza dei dati;
- Consegnare a persone non autorizzate dal Responsabile della sicurezza dei dati, stampe o altro materiale riguardante dati oggetto di trattamento.

Durante l'orario di servizio gli incaricati hanno il compito di controllare direttamente i sistemi, i P.C. installati e l'accesso negli stessi uffici allo scopo di impedire intrusioni o danneggiamenti. In orario non di servizio, esistono i registri di accesso negli uffici da compilare da chiunque estraneo volesse accedervi. Inoltre sono state impartite istruzioni ai collaboratori scolastici in merito al comportamento da tenere per limitare l'accesso negli uffici e assicurare che eventuali accessi siano registrati.

#### **1.6. MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO**

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, è stata definita una procedura di periodica esecuzione di copie di sicurezza dei dati trattati come specificato nello schema sopra. Sono state perciò acquisite licenze di uso per software antivirus, nonché sistemi di firewall con verifica di idoneità e costante aggiornamento. I documenti cartacei sono conservati negli armadi con serrature non disponibili ai terzi o a personale non autorizzato.

Per ogni banca dati, vengono predisposte le istruzioni di copia, verifica e ripristino dei dati. In particolare per ogni banca dati vengono definite le seguenti specifiche:

- Il tipo di supporto da utilizzare per le copie di sicurezza;
- Il numero di copie di sicurezza dei dati effettuate ogni volta;
- La modalità di controllo delle copie di sicurezza;
- Il nome dell'incaricato per l'effettuazione delle copie di sicurezza dei dati;
- Le istruzioni per l'effettuazione delle copie di sicurezza;
- Le istruzioni per il ripristino delle copie di sicurezza dei dati.

In sintesi si rappresenta nella tabella 3 che segue la procedura di copia, verifica e ripristino dei dati per ogni p.c. o terminale di collegamento a server. Tenendo conto che le segreterie sono collegate in rete, le copie di sicurezza del programma principale di gestione (SISSI) si effettuano sul Server.

La procedura per la copia di sicurezza di altri programmi è come nella tabella 3b.

**Tabella 3 Procedure di copia, verifica e ripristino per ogni singola unità contenente dati**

Uffici	Applicativo	Sistema operativo	Supporti magnetici	Procedura di copia	Procedura di verifica	Ripristino
Le segreterie Dell'Istituto e ufficio DSGA	Sissi in rete	Server Windows2000	Cassette e Tipo DAT	Procedura di back-up Windows 2000 server	Procedura di back-up Windows 2000 server	Procedura di back-up Windows 2000 server

**Tabella 3b - Procedure di copia, verifica e ripristino per ogni singola unità contenente dati gestiti con Office o altri programmi diversi da Sissi**

Uffici	Applicativo	Sistema operativo	Supporti magnetici	Procedura di copia	Procedura di verifica	Ripristino
- Ufficio del Dirigente scolastico - Ufficio del Direttore S.G.A - Segreterie e dell'Istituto	Office	Server Windows2000	Salvataggio giornaliero da parte degli uffici nella cartella condivisa chiamata "GESTIONE"	Procedura di back-up Windows 2000 server	Procedura di back-up Windows 2000 server	Procedura di back-up Windows 2000 server

Con riferimento invece al contenuto ed alle competenze in tema di copia, verifica e ripristino, le soluzioni organizzative adottate presso l'Istituto sono sintetizzate nella seguente tabella:

Tabella 4 Salvataggio dei dati

<b>SALVATAGGIO</b>		<b>CRITERI INDIVIDUATI PER IL SALVATAGGIO</b>	<b>UBICAZIONE DI CONSERVAZIONE DELLE COPIE</b>	<b>STRUTTURA OPERATIVA INCARICATA DEL SALVATAGGIO</b>
<b>STRUTTURA</b>	<b>DATI SENSIBILI O GIUDIZIARI CONTENUTI</b>			
Ufficio del Dirigente scolastico		Salvataggio dati mensile	Ufficio amministrativo e elaborazione dati con serratura con chiavi distribuite fra i soli autorizzati	Incaricato copie di sicurezza
Uffici del personale	- Stato di salute (dispense dal servizio, aspettative) - adesione a sindacati - origine razziale o etnica - confessione religiosa	Salvataggio dati settimanale/giornaliero.	Ufficio amministrativo e elaborazione dati con serratura con chiavi distribuite fra i soli autorizzati	Incaricato copie di sicurezza
Ufficio amministrativo e elaborazione dati.	- dati giudiziari inerenti imprese interessate ad attività negoziali, stipendi e dati fiscali del personale	Salvataggio dati settimanale/giornaliero	Ufficio amministrativo e elaborazione dati con serratura con chiavi distribuite fra i soli autorizzati	Incaricato copie di sicurezza

Ufficio Alunni	<ul style="list-style-type: none"> <li>- Stato di salute –</li> <li>- Situazione --di handicap-</li> <li>- origine razziale o etnica-</li> <li>- confessione religiosa</li> <li>- situazione economica</li> </ul>	Salvataggio dati settimanale/giornaliero	Ufficio amministrativo e elaborazione dati con serratura con chiavi distribuite fra i soli autorizzati	Incaricato copie di sicurezza
Ufficio protocollo, patrimonio e Servizi strumentali agli organi collegiali	<ul style="list-style-type: none"> <li>- Stato di salute</li> <li>- origine razziale o etnica</li> <li>-confessione religiosa</li> </ul>	Salvataggio dati giornaliero per il protocollo e settimanale per gli altri	Ufficio amministrativo e elaborazione dati con serratura con chiavi distribuite fra i soli autorizzati	Incaricato copie di sicurezza
Ufficio del Direttore S.G.A.	<ul style="list-style-type: none"> <li>- dati giudiziari inerenti imprese interessate ad attività negoziali, stipendi e dati fiscali del personale</li> </ul>	Salvataggio dati settimanale/giornaliero	Ufficio amministrativo e elaborazione dati con serratura con chiavi distribuite fra i soli autorizzati	Incaricato copie di sicurezza

Con riferimento alle procedure di prove di ripristino, l'Istituto ha adottato le seguenti modalità:

**Tabella 5 Prove di ripristino dei dati**

<b>RIPRISTINO (in seguito a distruzione o danneggiamento)</b>		
<b>DATA BASE/ARCHIVIO</b>	<b>SCHEDA OPERATIVA</b>	<b>PIANIFICAZIONE DELLE PROVE DI RIPRISTINO</b>
Ufficio del Dirigente scolastico	Un back up dei dati trattati e dei documenti presenti sull'HD su una copia di supporti conservata dall'incaricato delle copie delle banche dati nell'ufficio amministrativo e elaborazione dati.	Semestrale
Uffici del personale	Come sopra	Semestrale
Ufficio amministrativo e elaborazione dati	Come sopra	Semestrale
Ufficio alunni	Come sopra	Semestrale
Ufficio Protocollo, Patrimonio e servizi strumentali agli organi collegiali	Come sopra	Semestrale
Ufficio del Direttore S.G.A.	Come sopra	Semestrale

### **1.7. PROGRAMMA DEGLI INTERVENTI FORMATIVI DEL PERSONALE**

Il Direttore S.G.A. ha partecipato alle iniziative formative organizzate dalla direzione regionale per la Toscana in materia di sicurezza dei dati personali.

L'Istituto tenendo ben presente quanto segue:

- 1) il contenuto del corso come indicato nel punto 19 dell'Allegato B del D. Lgs. 196/2003;
- 2) Ente organizzatore del corso;
- 3) Problemi logistici, visti i numeri di sedi in cui l'Istituto è composto, privilegerà corsi organizzati dal Ministero o dall'Ufficio Scolastico Regionale e quindi senza costi a carico dell'Istituto. Al momento per i corsi necessari per adempiere agli obblighi di formazione del personale per motivi logistici, il Direttore S.G.A. organizzerà i corsi interni per tutto il personale dell'istituto con calendario come indicato nella tabella 6.

**Tabella 6 Pianificazione degli interventi formativi**

<b>OGGETTO DEL CORSO DI FORMAZIONE</b>	<b>OBIETTIVO FORMATIVO</b>	<b>PERSONALE INTERESSATO</b>	<b>NUMERO DI PERSONALE INTERESSATO</b>	<b>PERSONALE FORMATO/DA FORMARE NEL CORSO DELL'ANNO</b>	<b>CALENDARIO</b>
L'adempimento dell'obbligo di aggiornamento del DPS	Porre in condizione il personale competente di adempiere entro il 30.6.2005 all'obbligo di aggiornamento del DPS	Tutto il personale della segreteria (titolari di credenziali di autenticazione e (codice identificativo e password riservata personale) Tutti i collaboratori scolastici.	9 personale della segreteria 27 collaboratori scolastici e tutti i docenti	tutti	Concordato con il personale
Programma del corso	Obiettivo da realizzare	Personale coinvolto			Calendario
gli adempimenti e gli obblighi in materia di privacy (ivi incluse le misure di sicurezza per gli archivi cartacei)	Mantenimento del richiesto grado di conoscenza dell'intero impianto della normativa in materia di privacy, anche ai fini delle misure di sicurezza da adottare per gli archivi cartacei.	il personale di segreteria, i docenti e i collaboratori scolastici			Entro il 15.5.2005

Privacy e diritto di accesso nelle istituzioni scolastiche	Fornire un quadro coordinato dei diritti (di accesso e alla riservatezza) riconosciuti all'utenza dalla vigente legislazione, in rapporto ai doveri gravanti sulle strutture scolastiche	il personale di segreteria			Entro il 30.06.2005
Esame della casistica ricorrente nell'attività di ufficio, alla luce delle sentenze del giudice amministrativo e dei pronunciamenti del Garante	Aggiornare il personale sull'evoluzione e dell'interpretazione della normativa intervenuta nel corso dell'anno	il personale di segreteria			Entro il 15.12.2005

## **1.8. TRATTAMENTI DI DATI PERSONALI SENSIBILI O GIUDIZIARI CON STRUMENTI ELETTRONICI AFFIDATI ALL'ESTERNO.**

L'Istituto non ha in programma l'esternalizzazione di trattamenti dei dati.

## **1.9. ATTI E DOCUMENTI NON IN FORMATO ELETTRONICO, ARCHIVI CARTACEI**

I trattamenti di dati personali con strumenti diversi da quelli elettronici (fascicoli personali) sono effettuati dagli incaricati seguendo le istruzioni ad essi impartite con il documento di nomina. I registri personali dei docenti e i registri di classi fanno parte di questo tipo di trattamento. Gli atti e i documenti in cartacei contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti. I medesimi atti e documenti sono controllati e custoditi dagli incaricati in maniera che ad essi non accedano persone prive di autorizzazione.

L'accesso agli archivi cartacei contenenti dati sensibili o giudiziari è consentito solamente alle persone preventivamente autorizzate.

## **1.10 SISTEMA DI AUTORIZZAZIONE.**

In considerazione delle esigenze organizzative dell'istituto, per il cui ordinario funzionamento è indispensabile assicurare una certa interscambiabilità funzionale degli incaricati, non è stato adottato un sistema di autorizzazione al di fuori del sistema di credenziali di autenticazione (Password).

## **1.11. OBBLIGO DI AGGIORNAMENTO PERIODICO DEL DPS**

Nel rispetto del disposto dell'art. 34, lettera g del D.Lgs. 196/2003, il presente documento programmatico sulla sicurezza è soggetto all'aggiornamento in caso di necessità ed è sottoposto ad una revisione annuale, entro la scadenza del 31 marzo di ciascun anno, come previsto nel punto 19 dell'allegato B dello stesso decreto (Disciplinare tecnico in materia di misure minime di sicurezza).

Gli allegati al presente documento ne formano parte integrante.

Il presente documento è aggiornato al 31/08/2005

Il Titolare del trattamento  
(Prof.ssa Somigli Stefania)

Il Responsabile del trattamento  
(Kingsley Franks)

## **ALLEGATI**

### **2.0 DEFINIZIONI**

#### **2.1 Trattamento**

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distribuzione di dati, anche se non registrati in una banca di dati.

#### **2.2 Dato personale**

Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

#### **2.3 Dati sensibili**

I dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose filosofiche oppure di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale.

#### **2.4 Dati giudiziari**

I dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r a u), del DPR 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

#### **2.5 Titolare**

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

#### **2.6 Responsabile**

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

#### **2.7 Incaricati**

Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

## **2.8 Interessato**

La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

## **2.9 Comunicazione**

Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

## **2.10 Diffusione**

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

## **2.11 Dato anonimo**

Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

## **2.12 Blocco**

La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

## **2.13 Banca dati**

Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

## **2.14 Comunicazione elettronica**

Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

## **2.15 Misure minime**

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

### **2.1.16 Strumenti elettronici**

Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

### **2.17 Autenticazione informatica**

L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta della identità.

### **2.18 Credenziali di autenticazione**

I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

### **2.19 Parola chiave**

Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

### **2.20 Profilo di autorizzazione**

L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

### **2.21 Sistema di autorizzazione**

L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

### **3. DIRITTI DELL'INTERESSATO**

#### **3.1 Diritto di accesso ai dati personali**

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
  - a) dell'origine dei dati personali;
  - b) delle finalità e modalità del trattamento;
  - c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
  - d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5 comma 2;
  - e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
  - a) l'aggiornamento, la rettificazione, ovvero, quando vi ha interesse, l'integrazione dei dati;
  - b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati;
  - c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
  - a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
  - b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

### 3.2 Esercizio dei diritti

1. I diritti di cui all'art. 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, al quale è fornito idoneo riscontro senza ritardo.
2. I diritti di cui all'art. 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'art. 145, se i trattamenti di dati personali sono effettuati:
  - a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni in materia di riciclaggio;
  - b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;
  - c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
  - d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
  - e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
  - f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;
  - g) per ragioni di giustizia, presso gli uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;
  - h) ai sensi dell'art. 53, fermo restando quanto previsto dalla legge 1° Aprile 1981, n. 121.
3. Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f), provvede nei modi di cui agli articoli 157, 158, 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160.
4. L'esercizio dei diritti di cui all'art. 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché la indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

### 3.3 Modalità d'esercizio

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quanto riguarda l'esercizio dei diritti di cui all' articolo 7, commi 1 e 2, la richiesta

può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato e del responsabile.

2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.
3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
4. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.
5. La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con l'intervallo non minore di novanta giorni.

### **3.4 Riscontro all'interessato**

1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:
  - a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
  - b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.
2. I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.
3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'art. 84, comma 1.
4. Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

5. Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati relativi all'interessato.
6. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.
7. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.
8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente.  
Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.
9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

#### **4. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del codice)**

##### **4.1 Trattamenti con strumenti elettronici**

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dello incaricato, in caso di trattamento con strumenti elettronici.

##### **4.2 Sistema di autenticazione informatica**

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentono il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è 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 contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente allo incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare

chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o di impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

#### **4.3 Sistema di autorizzazione**

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, 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.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

#### **4.4 Altre misure di sicurezza**

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

#### **4.5 Documento programmatico sulla sicurezza**

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
- 19.1. l'elenco dei trattamenti di dati personali;
  - 19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
  - 19.3. l'analisi dei rischi che incombono sui dati;
  - 19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
  - 19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
  - 19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli 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. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
  - 19.7. la 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;
  - 19.8. i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

#### **4.6 Ulteriori misure in caso di trattamento di dati sensibili o giudiziari**

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per 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.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente allo interno di locali protetti accessibili ai soli incaricati dei trattamenti e ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

#### **4.7 Misure di tutela e garanzia**

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dello intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

#### **4.8 Trattamenti senza l'ausilio di strumenti elettronici**

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

## 5. Gli incarichi

- 5.1 Lettera di incarico al Responsabile della sicurezza dei dati personali
- 5.2 Lettera di nomina al Responsabile di specifico trattamento di dati personali  
Ufficio Alunni
- 5.3 Lettera di nomina al Responsabile di specifico trattamento di dati personali  
Ufficio Amministrazione e elaborazione dati
- 5.4 Lettera di nomina al Responsabile di specifico trattamento di dati personali  
Ufficio Personale
- 5.5 Lettera di nomina al Responsabile di specifico trattamento di dati personali  
Ufficio protocollo e patrimonio
- 5.6 Lettera di nomina dell'incaricato della custodia delle copie delle credenziali
- 5.7 Lettera di nomina dell'incaricato della gestione e della manutenzione degli  
strumenti elettronici
- 5.8 Lettera di nomina dell'incaricato delle copie di sicurezza delle banche dati
- 5.9 Lettera di incarico per il trattamento dei dati ufficio amministrazione e  
elaborazione dati
- 5.10.1 Lettere di incarico per il trattamento dei dati ufficio Alunni
- 5.10.2 Lettere di incarico per il trattamento dei dati ufficio Alunni
- 5.10.3 Lettere di incarico per il trattamento dei dati ufficio Alunni
- 5.10.4 Lettere di incarico ai docenti per il trattamento dei dati ufficio Alunni – Registri  
di classe e degli insegnanti
- 5.11.1 Lettere di incarico per il trattamento dei dati ufficio personale
- 5.11.2 Lettere di incarico per il trattamento dei dati ufficio personale
- 5.11.3 Lettere di incarico per il trattamento dei dati ufficio personale
- 5.12.1 Lettere di incarico per il trattamento dei dati ufficio protocollo e patrimonio
- 5.12.2 Lettere di incarico per il trattamento dei dati ufficio protocollo e patrimonio
- 5.13.1 Lettera di incarico per il controllo degli accessi alle aree e ai locali addebiti al  
trattamento dei dati personali
- 5.13.2 Lettera di incarico per il controllo degli accessi alle aree e ai locali addebiti al  
trattamento dei dati personali
- 5.13.3 Lettera di incarico per il controllo degli accessi alle aree e ai locali addebiti al  
trattamento dei dati personali
- 5.13.4 Lettera di incarico per il controllo degli accessi alle aree e ai locali addebiti al  
trattamento dei dati personali
- 5.13.5 Lettera di incarico per il controllo degli accessi alle aree e ai locali addebiti al  
trattamento dei dati personali