



LICEO ARTISTICO STATALE “CARAVAGGIO”

Via Prinetti, 47 - 20127 MILANO

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

*REDATTO AI SENSI E PER GLI EFFETTI DELL'ARTICOLO 34, COMMA 1, LETTERA G)
DEL D.LGS 196/2003, E DEL DISCIPLINARE TECNICO ALLEGATO AL MEDESIMO
DECRETO SUB B)*

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Scopo del presente Documento Programmatico sulla Sicurezza (“DPS”) è quello di delineare il quadro delle misure di sicurezza, organizzative, fisiche e informatiche, adottate e da adottarsi per il trattamento dei dati personali effettuato dal Liceo Artistico Statale “Caravaggio”, con sede in Milano, via Prinetti 47, nella persona del Preside quale proprio legale rappresentante (il “Titolare”).

=====

Conformemente al disposto del Disciplinare Tecnico, allegato al D.Lgs. 196/2003, punto 19, nel presente documento sono fornite idonee informazioni riguardanti:

1. l'elenco dei trattamenti di dati personali;
2. la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati e previsione di interventi formativi rivolti agli incaricati del trattamento;
3. l'analisi dei rischi che incombono sui dati;
4. le misure necessarie per garantire l'integrità e la disponibilità dei dati nonché la protezione di aree e locali rilevanti ai fini della relativa custodia ed accessibilità;
5. i criteri e le modalità di ripristino dei dati in seguito a distruzione o danneggiamento;
6. i criteri da adottare, per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno.

INDICE

CAPITOLO 1 - ELENCO DEI TRATTAMENTI DEI DATI PERSONALI	3
1.1 MAPPATURA DEI DATI TRATTATI.....	3
1.2 CARATTERISTICHE DI AREE, LOCALI E STRUMENTI CON CUI SI EFFETTUANO I TRATTAMENTI	1
CAPITOLO 2 - MANUALE INTERNO DELLA PRIVACY	2
2.1 RESPONSABILE DEL TRATTAMENTO	2
2.2 GLI INCARICATI DEL TRATTAMENTO	2
2.3 DISPOSIZIONI RELATIVE AL TRATTAMENTO DEI DATI	2
2.4 INFORMATIVA	3
2.5 CONSENSO	3
2.5 DIRITTI DEGLI INTERESSATI	3
2.6 FORMAZIONE	4
3. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI	5
3.1. RISCHI IN FUNZIONE DELLA TIPOLOGIA DEI DATI.....	5
3.2. RISCHI IN FUNZIONE DELLE MODALITÀ DI TRATTAMENTO ADOTTATE	6
STRUMENTI UTILIZZATI.....	6
4. MISURE ATTE A GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI	7
4.1 PROTEZIONE DI AREE E LOCALI; ARCHIVIAZIONE E CUSTODIA.....	7
4.2 LE MISURE LOGICHE DI SICUREZZA	7
4.2.1 Autenticazione.....	8
4.2.2. Autorizzazione:.....	8
4.2.3 Protezione degli elaboratori e dei dati ivi contenuti	9
Custodia ed utilizzo dei supporti rimovibili contenenti dati personali.....	9
5. CRITERI E MODALITÀ DI RIPRISTINO DEI DATI.....	9
6. AFFIDAMENTO DI DATI PERSONALI ALL'ESTERNO	10
7. DICHIARAZIONI D'IMPEGNO E FIRMA	10
ALLEGATI	11

CAPITOLO 1 - ELENCO DEI TRATTAMENTI DEI DATI PERSONALI

L'elenco dei trattamenti dei dati personali posti in essere dal Titolare è costituito dalla mappatura di tali dati e dalla descrizione delle aree, locali e strumenti con i quali si effettuano detti trattamenti.

1.1 Mappatura dei dati trattati

La mappatura dei dati trattati dal Titolare, con l'indicazione della tipologia dei dati, della eventuale sensibilità degli stessi, del tipo di trattamento, dell'esistenza di previsioni normative in merito, e del tipo di strumento utilizzato, è riportata nelle tabelle che seguono.

MAPPA DEL TRATTAMENTO DEI DATI

Tipologia del dato ¹		Dato sensibile (S/N) ²	Tipo di trattamento	Trattamento previsto per espressa norma di legge (L) o per altre funzioni istituzionali (F) ³	Trattamento con sistemi elettronici (E) o cartaceo (C) ⁴
Dati allievi (1)	Dati anagrafici e titoli	N	raccolta, organizzazione, conservazione, consultazione, modificazione, comunicazione	L	E/C
	Scelta ora di religione	S	raccolta, organizzazione, conservazione	L	E/C
	Portatori di handicap	S	raccolta, organizzazione, conservazione	L	E/C
	Certificati medici	S	raccolta, conservazione	L	E/C
<u>Dati allievi (2)</u>	Votazione / andamento scolastico	N	raccolta, organizzazione, conservazione, consultazione, elaborazione, modificazione, raffronto, utilizzo, comunicazione, diffusione	L	E/C
	Nazionalità	S	raccolta, conservazione	L	E/C
	Stato di Famiglia	N	raccolta, conservazione	L	E/C
	Redditi / Sussidi / Coordinate bancarie	N	raccolta, organizzazione, conservazione, consultazione, elaborazione, modificazione, raffronto, utilizzo, comunicazione	L	E/C

¹ Tipologia di dati.

² S = dati sensibili; N = altri dati personali.

³ L = trattamento previsto espressamente da una norma di legge; F = trattamento previsto per altre funzioni istituzionali.

⁴ E = trattamento mediante strumenti elettronici. C = trattamento mediante strumenti cartacei; E/C = trattamento mediante strumenti sia elettronici che cartacei.

Tipologia del dato		Dato sensibile (S/N)	Tipo di trattamento	Trattamento previsto per espressa norma di legge (L) o per altre funzioni istituzionali (F)	Trattamento con sistemi elettronici (E) o cartaceo (C)
<u>Dati allievi (3)</u>	Registro assenze	N	raccolta, organizzazione, conservazione, consultazione, raffronto, utilizzo, comunicazione	L	E/C
	Trattamenti occasionali	--	--	--	--
<u>Dati personale dipendente (1)</u>	Dati anagrafici e titoli	N	raccolta, organizzazione, conservazione, consultazione, modificazione, utilizzo	L	E/C
	Redditi / Coordinate bancarie	N	Raccolta, conservazione, modificazione, utilizzo, comunicazione	L	E/C
	Dati relativi allo stato di salute permanente	S	raccolta, organizzazione, conservazione, consultazione, utilizzo	L	E/C
	Certificati medici	S	raccolta, organizzazione, conservazione, utilizzo	L	E/C
	Assenze / Ferie	N	raccolta, organizzazione, conservazione, utilizzo	L	E/C
<u>Dati personale dipendente (2)</u>	Adesione a scioperi	S	Raccolta, conservazione, consultazione, utilizzo, cancellazione	L	E/C
	Dati soggetti esterni ⁵	N	Raccolta, conservazione, elaborazione, raffronto, utilizzo, comunicazione	L	E/C

⁵ Dati relativamente ai quali viene effettuata una graduatoria, comunicata al Provveditorato agli Studi.

Tipologia del dato		Dato sensibile (S/N)	Tipo di trattamento	Trattamento previsto per espressa norma di legge (L) o per altre funzioni istituzionali (F)	Trattamento con sistemi elettronici (E) o cartaceo (C)
<u>Dati fornitori</u>	Anagrafica fornitori	N	raccolta, organizzazione, conservazione, consultazione, modificazione, selezione, raffronto, utilizzo	F	E/C
	Rapporti contrattuali in essere	N	raccolta, organizzazione, conservazione, consultazione, modificazione	F	E/C
<u>Gestione siti internet</u> ⁶	Dati generici	N	raccolta, organizzazione, conservazione, consultazione, elaborazione, modificazione	F	E

⁶ I siti attualmente gestiti dal Liceo Artistico Statale “Caravaggio” sono: www.liceocaravaggio.com e www.artinrete.org.

1.2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti

Il trattamento dei dati personali avviene all'interno della sede del Titolare.

Il trattamento dei dati personali avviene con i **seguenti strumenti**:

A – Schedari ed altri supporti cartacei

I supporti cartacei, ivi inclusi quelli contenenti immagini, sono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati, una volta terminato il ciclo lavorativo, come segue:

- **Archivio 1**, localizzato nei locali della Segreteria e della Presidenza, nel quale vengono raccolti i dati di natura amministrativa (anche sensibili) necessari per lo svolgimento delle attività istituzionali del Titolare, nonché i registri di classe.
- **Archivio 2**, localizzato nella cantina della sede del Titolare, nel quale si raccolgono le pratiche e gli schedari relativi all'archivio storico.
- **Archivio 3**, localizzato presso gli armadietti dei professori, in cui si raccolgono i registri personali di ciascun professore.

B – Elaboratori in rete con accesso privato

Per elaboratori in rete con accesso privato si intendono quegli elaboratori, per ciascuno dei quali è identificato uno specifico incaricato, che sono collegati tramite una rete cui possono accedere unicamente i soggetti autorizzati interni all'organizzazione del Titolare, nonché i server cui tali elaboratori si appoggiano.

Essi sono costituiti da:

- numero 6 postazioni fisse ("**Elaboratori 1-6**"), dislocate nei locali della Segreteria, contenenti dati di natura amministrativa (anche sensibili) necessari per lo svolgimento delle attività istituzionali del Titolare;
- numero 2 server, in rete tra loro:
 - **Server 1** (o "Centrale"), dislocato presso i locali della Segreteria, dotato di accesso ad internet ed e-mail;
 - **Server 2** (o "Amministrativo"), dislocato presso i locali della Segreteria, dotato di postazione propria, contenente dati di natura amministrativa (anche sensibili) necessari per lo svolgimento delle attività istituzionali del Titolare.

C – Elaboratori in rete con accesso pubblico

Per elaboratori in rete con accesso pubblico si intendono quelli accessibili, anche solo per alcuni archivi, da parte di soggetti esterni all'organizzazione del Titolare.

Essi sono costituiti da:

- **Server 3**, localizzato presso i locali della Segreteria, nel quale sono trattate valutazioni, assenze, dati anagrafici degli allievi.

CAPITOLO 2 - MANUALE INTERNO DELLA PRIVACY

2.1 Responsabile del trattamento

Il Titolare nomina per ciascun anno scolastico il Responsabile ai sensi dell'art. 29 D.Lgs. 196/2003, individuandolo tra i soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle disposizioni normative in materia. La nomina del responsabile e la relativa accettazione da parte di quest'ultimo avvengono con atto separato, allegato al DPS.

Il Titolare, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative, di sicurezza, e delle proprie istruzioni.

Compiti del Responsabile sono:

- Gestire i trattamenti, attenendosi alle istruzioni impartite dal Titolare.
- Supervisionare e provvedere al mantenimento in efficienza delle misure di sicurezza, conformemente a quanto previsto dagli artt. 31 e 33 Dlgs 196/2003.
- Garantire il soddisfacimento dei diritti esercitabili dai soggetti interessati, ai sensi degli articoli da 7 a 10 Dlgs 196/2003.
- Aggiornare gli elementi descrittivi del DPS.
- Nominare Incaricati del trattamento ai sensi dell'art. 30 D.Lgs. 196/2003.
- Fornire agli Incaricati le indicazioni di carattere operativo necessarie al corretto adempimento dei relativi incarichi.

2.2 Gli Incaricati del trattamento

Il trattamento dei dati personali può essere effettuato esclusivamente da Incaricati ai sensi dell'art. 30 D.Lgs. 196/2003 (gli "Incaricati") che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite.

La designazione degli Incaricati avviene a cura del Titolare o del Responsabile:

- per iscritto, individuando puntualmente l'ambito del trattamento consentito, ovvero
- mediante la documentata preposizione del soggetto ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

I docenti sono Incaricati del trattamento dei dati inerenti all'attività didattica.

La lista degli Incaricati ovvero delle unità per le quali è individuato l'ambito di trattamento di dati personali consentito, è allegata al DPS ed è aggiornata a cura del Responsabile.

2.3 Disposizioni relative al trattamento dei dati

1. I dati personali oggetto di trattamento sono:
 - a) trattati in modo lecito e secondo correttezza;
 - b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in termini compatibili con detti scopi;
 - c) esatti e periodicamente aggiornati;
 - d) pertinenti, completi e non eccedenti le finalità per le quali sono raccolti e trattati;
 - e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
2. I dati segnalati nella Mappa dei Rischi di cui al cap. 3 del DPS come meritevoli di particolare attenzione sono trattati con maggiori cautele rispetto a quanto è previsto per i dati

di natura comune; il Responsabile fornisce specifiche indicazioni al riguardo, con riferimento alle singole ipotesi.

3. I documenti contenenti dati personali sono custoditi ed archiviati in conformità alle misure di sicurezza di cui al cap. 4 del DPS.
4. Gli strumenti elettronici ed i documenti cartacei contenenti dati personali non devono essere lasciati incustoditi e accessibili.
5. In caso di cessazione di un trattamento, i dati sono (i) distrutti, (ii) ceduti ad altro titolare nel rispetto della normativa, (iii) conservati e non destinati alla comunicazione sistematica o alla diffusione.
6. Gli addetti alla gestione e manutenzione del sistema informativo non sono autorizzati ad effettuare alcun trattamento sui dati personali contenuti negli strumenti elettronici, fatta eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

2.4 Informativa

1. Ogni trattamento di dati personali da parte del Titolare, del Responsabile, e degli Incaricati, è consentito esclusivamente per lo svolgimento delle funzioni istituzionali del Liceo Artistico Statale “Caravaggio”.
2. Il Titolare informa per iscritto ogni interessato relativamente alle finalità e le modalità del trattamento cui sono destinati i dati; alla natura obbligatoria o facoltativa del conferimento dei dati; alle conseguenze di un eventuale rifiuto di rispondere; ai soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; ai diritti riconosciuti all'interessato ai sensi dell'art.7 D.Lgs. 196/2003; agli estremi identificativi del Titolare e del Responsabile.
2. L'informativa è resa al momento di instaurazione del rapporto, salvo che si renda necessario il rinnovamento della stessa per intervenute modifiche del trattamento comunicato.

2.5 Consenso

1. Il Titolare, in qualità di soggetto pubblico, non deve richiedere il consenso degli interessati per effettuare il trattamento dei dati personali, ai sensi dell'art. 18 D.Lgs. 196/2003.
2. Qualora specifiche circostanze relative a particolari trattamenti lo consiglino, resta in facoltà del Titolare richiedere il consenso espresso dell'interessato a detti trattamenti.

2.5 Diritti degli interessati

1. Conformemente alle previsioni di cui all'art. 7 D.Lgs. 196/2003, ogni interessato ha diritto di ottenere conferma dell'esistenza o meno di dati personali riguardandolo, e la loro comunicazione. Inoltre, ha diritto di ottenere l'indicazione dell'origine dei dati personali, delle finalità e modalità del trattamento, della logica applicata in caso di trattamento effettuato mediante strumenti elettronici, degli estremi identificativi del Titolare e del Responsabile, dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di Incaricati. L'interessato ha infine diritto di ottenere l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; la cancellazione, la trasformazione in forma anonima o il blocco dei dati qualora questi fossero trattati in violazione di legge; l'attestazione che le operazioni di cui sopra sono state portate a conoscenza di coloro cui i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento sia impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

2. Nel caso di esercizio da parte di un interessato dei diritti di cui all'articolo 7 D.Lgs. 196/2003, ne viene prontamente informato il Responsabile, il quale verifica l'identità dell'interessato sulla base di idonei elementi di valutazione. Qualora per conto dell'interessato agisse una persona terza, alla stessa è richiesto di allegare copia della procura, ovvero della delega sottoscritta e unitamente a copia di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente od un'associazione, la richiesta deve essere avanzata dal legale rappresentante o da altra persona legittimata allo scopo.

3. I dati richiesti sono estratti a cura del Responsabile o degli Incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici. Se vi è richiesta in tal senso, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica; nel caso in cui l'estrazione dei dati risulti particolarmente difficoltosa, il riscontro può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.
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.
La comunicazione dei dati non comprende i dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.
Qualora non risulti confermata l'esistenza di dati riguardanti l'interessato, può essere richiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata.

2.6 Formazione

Il Titolare prevede espressamente lo svolgimento di appositi **interventi formativi nei confronti degli Incaricati del trattamento**, finalizzati in particolare ad illustrare:

- profili della disciplina sulla protezione dei dati personali e delle conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati personali;
- misure per prevenire eventi dannosi;
- aggiornamento sulle misure di sicurezza adottate dal titolare.

Tali interventi formativi hanno luogo al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni implicanti modifiche rilevanti rispetto al trattamento di dati personali, nonché in occasione dell'introduzione di nuovi strumenti che implicino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi sono curati dal Responsabile, che a tal fine può avvalersi anche di soggetti esterni.

3. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

La mappatura dei rischi relativi al trattamento di dati da parte del Liceo Artistico Statale “Caravaggio” è effettuata tenendo in considerazione (i) i rischi relativi ai dati in funzione della relativa tipologia, e (ii) i rischi relativi alle specifiche modalità di trattamento adottate.

3.1. Rischi in funzione della tipologia dei dati

Il grado di rischio dipendente dalla tipologia dei dati trattati dal Titolare viene qui definito combinando l'intensità del rischio (derivante dal possibile interesse da parte di terzi ad accedervi) con la pericolosità del trattamento (valutata in funzione del danno per il soggetto cui i dati si riferiscono in caso di accesso illegittimo).

INTENSITA' DEL RISCHIO (INTERESSE PER I TERZI)	ALTO			<ul style="list-style-type: none"> • Redditi/ sussidi/ coordinate bancarie allievi • Redditi / coordinate bancarie dipendenti • Adesione a scioperi dipendenti
	MEDIO	<ul style="list-style-type: none"> • Dati anagrafici e titoli allievi • Anagrafica fornitori 	<ul style="list-style-type: none"> • Scelta ora di religione allievi • Certificati medici allievi • Dati anagrafici e titoli dipendenti • Certificati medici dipendenti • Assenze/ferie dipendenti • Rapporti contrattuali in essere con fornitori 	<ul style="list-style-type: none"> • Portatori handicap allievi • Votazione/andamento scolastico allievi • Stato di salute permanente dipendenti
	BASSO	<ul style="list-style-type: none"> • Stato famiglia allievi • Registro assenze allievi • Dati soggetti esterni • Dati generici (gestione siti internet) 	<ul style="list-style-type: none"> • Nazionalità allievi 	
		BASSO	MEDIO	ALTO
PERICOLOSITA' DEL TRATTAMENTO (DANNO PER L'INTERESSATO)				

Dalla mappa sopra riportata si rileva come un grado di rischio alto è collegato al trattamento dei seguenti dati, il trattamento dei quali deve pertanto essere effettuato con particolare attenzione:

- Redditi/ sussidi/ coordinate bancarie allievi
- Coordinate bancarie dipendenti
- Adesione a scioperi dipendenti
- Portatori handicap allievi
- Votazione/andamento scolastico allievi
- Stato di salute permanente dipendenti

3.2. Rischi in funzione delle modalità di trattamento adottate

I rischi relativi alle specifiche modalità di trattamento adottate, vengono qui valutati sulla base degli strumenti impiegati per il trattamento, le cui componenti di rischio possono essere sinteticamente suddivise come segue.

1. Rischio di area, dipendente dal luogo dove gli strumenti sono ubicati. Tale rischio è legato sostanzialmente al verificarsi di eventi distruttivi (incendi, allagamenti, ecc.);
2. Rischio di guasti tecnici, particolarmente rilevante relativamente agli strumenti elettronici.
3. Rischio di penetrazione nelle reti di comunicazione e negli archivi.
4. Rischio legato ad atti volontari o ad errori umani da parte del personale appartenente al Liceo, o di terzi (allievi, fornitori).

Nella tabella che segue sono evidenziati i fattori di rischio cui sono soggetti gli strumenti con cui l'organizzazione procede al trattamento dei dati personali.

Il simbolo **B**, posto nella casella di intersezione, significa che l'esposizione al rischio appare modesta; il simbolo **M** significa che l'esposizione al rischio appare riconducibile alla media, il simbolo **A** significa che l'esposizione al rischio appare elevata

TIPI DI DATI TRATTATI							
Rischio d'area, legato al verificarsi di eventi distruttivi	M	M	M	M	M	M	M
Rischio d'area, legato all'accesso non autorizzato nei locali	M	B	M	B	B	M	B
Rischio di guasti tecnici di hardware, software e supporti	-	-	-	M	B	B	B
Rischio di penetrazione logica nelle reti di comunicazione	-	-	-	M	A	M	A
Rischio legato ad atti di sabotaggio e ad errori umani	M	B	A	M	M	M	B
	A1	A2	A3	Epv 1-6	Epv SC	Epv SAm	Epb
	STRUMENTI UTILIZZATI						

Legenda degli strumenti utilizzati per il trattamento:

- A:** Schedari ed altri supporti cartacei:
- **A1:** Archivio 1 (dati amministrativi)
 - **A2:** Archivio 2 (storico)
 - **A3:** Archivio 3 (registri professori)
- Epv 1-6:** Elaboratori 1-6, in rete con accesso privato
- Epv SC:** Server 1 Centrale, in rete con accesso privato
- Epv Sam:** Server 2 Amministrativo, in rete con accesso privato
- Epb:** Server 3, in rete con accesso pubblico

4. Misure atte a garantire l'integrità e la disponibilità dei dati

Nel presente capitolo sono descritte le misure atte a garantire:

- la protezione delle aree e dei locali, nei quali si svolge il trattamento dei dati personali, nonché la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici.

4.1 Protezione di aree e locali; archiviazione e custodia

Per quanto concerne il rischio d'area legato ad eventi di carattere distruttivo, i locali del Titolare sono protetti da dispositivi antincendio, a norma di legge.

Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati ai locali nei quali si svolge il trattamento, sono disposti i seguenti presidi:

- Presenza di custode all'ingresso del Liceo.
- Presenza di un sistema anti-intrusione.
- Specifico obbligo di vigilanza da parte del personale interno (Incaricati, personale ATAP) durante l'orario di apertura del Liceo.
- Espresso obbligo per gli Incaricati di non lasciare incustoditi gli Archivi. In particolare, nei locali della Segreteria dovrà essere sempre presente almeno un Incaricato o il Responsabile, durante l'orario lavorativo; in caso di impossibilità, detti locali devono essere chiusi a chiave. I locali della Segreteria devono essere chiusi a chiave al termine della giornata lavorativa.
- Armadi, cassette e simili nei quali sono conservati dati sensibili, anche su supporto informatico (*floppy*, CD-Rom), devono essere chiusi a chiave.
- Presenza di cassaforti nei locali della Segreteria, nelle quali sono custoditi i dati cartacei considerati a maggiore rischio. Le chiavi o codici di accesso relativi sono custoditi dal Titolare e/o dal Responsabile.
- Obbligo per gli Incaricati di riporre la documentazione contenente dati personali su supporto non elettronico negli Archivi al termine delle operazioni affidate.
- Obbligo per i docenti di riportare i registri di classe presso i locali della Segreteria al termine dell'ultima ora di lezione.
- Obbligo per i docenti di chiudere a chiave i propri registri personali nei rispettivi armadietti.

Il Titolare ed il Responsabile individuano le procedure più idonee finalizzate alla conservazione degli atti – laddove necessario – in archivi ad accesso selezionato, nonché alla identificazione degli Incaricati che vi accedono.

Su base annua, il Responsabile procede all'aggiornamento dell'ambito di trattamento consentito ai singoli Incaricati o alle unità organizzative.

Per l'anno 2004 sono previsti i seguenti interventi:

- Manutenzione del sistema antincendio nei termini previsti dalla normativa applicabile.
- Manutenzione del sistema anti-intrusione.
- Specifica formazione del personale, con particolare riferimento agli Incaricati.
- Verifica da parte del Responsabile del rispetto delle disposizioni del Titolare in materia di trattamento dei dati.

4.2 Le misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), sono adottati i seguenti presidi:

- Sistema di autenticazione informatica, che permette l'accesso ad ogni elaboratore esclusivamente ai soggetti autorizzati.
- Sistema di autorizzazione, che circoscrive le tipologie di dati cui gli Incaricati possono accedere, ed relativi i trattamenti .
- Sistema di protezione degli elaboratori e dei dati ivi contenuti da malfunzionamenti, attacchi informatici e programmi contenenti *virus*.
- Sistema di custodia ed utilizzo dei supporti rimovibili (floppy disk, CD-Rom, ecc.), nei quali siano contenuti dati personali.

Qualora le misure minime siano adottate avvalendosi di soggetti esterni alla struttura del Titolare, l'installatore rilascerà una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni del Discipinare Tecnico allegato al D.Lgs. 196/2003.

4.2.1 Autenticazione

L'accesso al trattamento è soggetto alla previa autenticazione informatica del soggetto operante tramite utilizzo di apposite credenziali di autenticazione ("Credenziali").

- Le Credenziali consistono in un codice per l'identificazione dell'Incaricato tramite una parola chiave, composta da almeno otto caratteri, riservata conosciuta solamente dal medesimo ovvero in un dispositivo di autenticazione in possesso e uso esclusivo dell'Incaricato. La parola chiave non contiene riferimenti agevolmente riconducibili all'Incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, ogni sei mesi. Il Responsabile conserva in cassaforte copia delle parole chiave assegnate.
- In caso di trattamento di dati sensibili e/o dati giudiziari la parola chiave è modificata ogni tre mesi.
- Ad ogni Incaricato sono assegnate o associate individualmente una o più Credenziali per l'autenticazione. La parola chiave, o altro codice per l'identificazione, non possono essere assegnati ad altri Incaricati, neppure in tempi diversi. Le Credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate. Le Credenziali sono disattivate anche in caso di perdita della qualità che consente all'Incaricato l'accesso ai dati personali.
- Gli Incaricati sono tenuti ad adottare le necessarie cautele per assicurare la segretezza della componente riservata della Credenziale e la diligente custodia degli eventuali dispositivi in loro possesso ed uso esclusivo.
- Gli Incaricati non devono lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. Qualora si renda necessaria una interruzione, detto strumento deve essere "ibernato".
- In caso di prolungata assenza o impedimento dell'Incaricato, qualora si renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, la disponibilità dei dati è assicurata dal Responsabile, con le modalità ritenute più opportune, che informa tempestivamente l'Incaricato dell'intervento effettuato.

Le disposizioni sul sistema di autenticazione non si applicano ai trattamenti di dati personali destinati alla diffusione.

4.2.2. Autorizzazione:

- Ogni Incaricato è abilitato a trattare esclusivamente i dati per i quali ha ricevuto l'incarico. Le autorizzazioni all'accesso vengono rilasciate e revocate dal Titolare ovvero dal Responsabile. Il profilo autorizzativo può essere definito per ogni singolo Incaricato, ovvero essere impostato per classi omogenee di Incaricati.

- Gli addetti alla gestione e manutenzione del sistema informativo non sono autorizzati ad effettuare alcun trattamento sui dati personali contenuti negli strumenti elettronici, fatta eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.
- Con cadenza periodica, almeno annuale, il Responsabile procede alla verifica della sussistenza delle condizioni per la conservazione dei profili di autorizzazione in capo agli Incaricati ed agli addetti alla manutenzione e gestione degli strumenti elettronici

Le disposizioni sul sistema di autorizzazione non si applicano ai trattamenti di dati personali destinati alla diffusione.

4.2.3 Protezione degli elaboratori e dei dati ivi contenuti

Per quanto riguarda la protezione degli elaboratori e dei dati ivi contenuti da malfunzionamenti, accessi non consentiti, e virus informatici, vengono adottate le seguenti misure.

- I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'articolo 615-*quinquies* del Codice Penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, tramite l'adozione di programmi "antivirus", che sono sottoposti ad aggiornamento almeno semestrale.
- I dati personali sono protetti contro il rischio di accesso abusivo di cui all'articolo 615-*ter* del codice penale (introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza, ovvero mantenimento nello stesso contro la volontà espressa o tacita di chi ha il diritto di escluderne i terzi), mediante l'impiego di idonei strumenti elettronici ("firewall"), sottoposti ad aggiornamento almeno semestrale.

Custodia ed utilizzo dei supporti rimovibili contenenti dati personali.

Per quanto concerne i supporti rimovibili (es. floppy disk, CD-Rom) contenenti dati personali, agli Incaricati è fatto obbligo di custodire ed utilizzare detti supporti in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti. In particolare, essi devono essere conservati in cassette o armadi chiusi a chiave e, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi, cancellati in modo definitivo.

Per l'anno 2004 sono previsti i seguenti interventi:

- Definizione e completa attuazione dei sistemi di autenticazione ed autorizzazione.
- Manutenzione ed aggiornamento dei programmi antivirus.
- Manutenzione ed aggiornamento dei programmi "firewall".
- Specifica formazione del personale, con particolare riferimento agli Incaricati.
- Verifica da parte del responsabile del rispetto delle disposizioni del Titolare in materia di trattamento dei dati.

5. Criteri e modalità di ripristino dei dati

Per i dati trattati con strumenti elettronici, è previsto il salvataggio di due copie di backup di tutti i dati contenuti sul Server 2 "Amministrativo". Dette copie sono effettuate su CD-Rom con cadenza almeno settimanale, su supporti differenti da quelli in cui sono contenuti i dati del salvataggio immediatamente precedente, e custodite a cura del Responsabile in luoghi protetti.

I dati trattati sugli Elaboratori sono salvati al termine di ogni sessione di lavoro, e comunque con frequenza almeno settimanale.

Il ripristino della disponibilità dei dati e dei sistemi è ulteriormente garantito tramite apposite intese con il soggetto incaricato della gestione del sistema.

5. Affidamento di dati personali all'esterno

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal D.Lgs. 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 del D.Lgs. 196/2003 e dal Disciplinare Tecnico, allegato sub b) al Decreto medesimo.

Per la generalità dei casi, in cui il trattamento di dati personali, di qualsiasi natura, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni al terzo destinatario di rispettare quanto prescritto per il trattamento dei dati personali dal Dlgs 196/2003, ovvero dalla direttiva 95/46/CE se il terzo destinatario non è italiano.

Nei casi in cui il trattamento affidato all'esterno abbia per oggetto dati sensibili o giudiziari, si procede alla stipula di apposite clausole contrattuali con il destinatario, che disciplinino gli aspetti legati alla gestione dei dati personali.

Nell'ipotesi in cui il trattamento, di dati sensibili o giudiziari, avvenga con strumenti elettronici, si esige inoltre che il destinatario rilasci la dichiarazione di avere redatto un proprio documento programmatico sulla sicurezza, col quale abbia recepito le disposizioni normative in tema di misure minime di sicurezza.

7. Dichiarazioni d'impegno e firma

Il presente Documento Programmatico della Sicurezza per il 2004/2005 è stato redatto, ai sensi dell'art. 34 del D.Lgs. 196/2003 e della regola 19 allegato B al codice dal Titolare in data 24 gennaio 2005

Lo stesso è portato a conoscenza di tutti gli Incaricati.

Rimane a disposizione degli organi competenti presso il Titolare.

E' valido a tutti gli effetti di legge fino al 31 marzo 2006

Milano, lì 24 gennaio 2005

IL DIRIGENTE SCOLASTICO
(Prof. G.B. MADERNA)

Firma del legale rappresentante del Titolare

Allegati

Allegato 1: Nomina del Responsabile del trattamento

Allegato 2: Lista delle unità organizzative per le quali è individuato per iscritto l'ambito del trattamento consentito.