I.I.S.S. "LEONARDO DA VINCI"
Prot. 0002842 del 16/05/2016
01-01 (Uscita)

Istituto di Istruzione Secondaria Superiore
LICEO SCIENTIFICO E CLASSICO STATALE
LEONARDO DA VINCI

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it
Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

Prot. n. 2842

Cassano delle Murge, 16/05/2016

Documento programmatico sulla sicurezza dei dati

Redatto in conformità del decreto legislativo 30 giugno 2003, n. 196 recante il Codice in materia di protezione di dati personali, in particolare gli art. 34 ss., nonché l'allegato B del suddetto D.lgs., contenente il Disciplinare tecnico in materia di misure minime di sicurezza;

Istituto di Istruzione Secondaria Superiore
LICEO SCIENTIFICO E CLASSICO STATALE
LEONARDO DAVINCI

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it
Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

Documento programmatico sulla sicurezza dei dati

Il Dirigente Scolastico

- Visto il decreto legislativo 30 giugno 2003, n. 196 recante il Codice in materia di protezione di dati personali, e segnatamente gli art. 34 ss., nonché l'allegato B del suddetto D.lgs., contenente il Disciplinare tecnico in materia di misure minime di sicurezza;
- Considerato che l'Istituzione Scolastica: IISS "Leonardo d" a Vinci, con sede in via Padre Angelo Centrullo, a Cassano delle Murge (Bari) in quanto dotata di un autonomo potere decisionale, ai sensi dell'art. 28 del d.lgs. n. 196 del 2004, deve ritenersi titolare del trattamento di dati personali;
- Atteso che la suddetta Istituzione scolastica è tenuta a prevedere ed applicare le misure minime di sicurezza di cui agli art. 31 e ss. del d.lgs. n. 196 del 2003,

Adotta

il presente Documento programmatico sulla sicurezza dei dati redatto ai sensi e per gli effetti dell'articolo 34, comma 1, lettera g) del D.lgs 196/2003 e del disciplinare tecnico allegato B

1. SCOPO DEL DOCUMENTO

Scopo di questo Documento Programmatico per la Sicurezza nel seguito indicato come DPS, è di delineare i criteri, le modalità operative e le misure organizzative, fisiche e logiche adottate dall'Istituto per garantire:

- la disponibilità delle informazioni per gli utenti del sistema, compatibilmente con i livelli di servizio;
- l'integrità delle informazioni, che quindi possono essere create, modificate o cancellate solo dalle persone autorizzate a svolgere tali operazioni;
- l'autenticità e la garanzia della provenienza dei dati;
- la riservatezza delle informazioni, che possono essere fruite solo dalle persone autorizzate.

In questo documento vengono definiti in particolare:

- l'elenco dei trattamenti di dati personali;
- i tipi di dati trattati;
- la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti;

- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- i modi per individuare e valutare i rischi;
- l'analisi dei rischi che incombono sui dati;
- le misure adottate per garantire l'integrità e la disponibilità dei dati e la sicurezza delle trasmissioni;
- nonché la protezione delle aree e dei locali;
- i criteri e le modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- gli interventi formativi previsti per gli incaricati del trattamento;
- i criteri da adottare in caso di affidamento del trattamento a soggetti esterni all'Istituto;
- le modalità di verifica e valutazione delle misure adottate.

Le indicazioni contenute nel presente documento devono essere utilizzate per gestire i rischi connessi alle attività di trattamento dei dati personali, sia in seno all'Istituto che da parte dei responsabili esterni.

2. CARATTERISTICHE DELL'ISTITUTO

Le persone

Gli alunni iscritti ai corsi sono n. 623

L'organico del personale:

- *docente*, compreso il personale che presta servizio anche in altre istituzioni scolastiche, è costituito da n. 68 Docenti;
- *A.T.A.* consta di n. 14 unità così distribuite:
  - n. 1 Direttore dei servizi generali ed amministrativi,
  - n. 4 assistenti amministrativi,
  - n. 2 assistenti tecnici,
  - n. 7 collaboratori scolastici.

Le strutture

La scuola è così articolata:
sede centrale sita nel comune di Cassano delle Murge, in Via Padre Angelo Centrullo, sn;
sede distaccata plesso "Platone" sita nel comune di Cassano delle Murge, in Viale Cinque Maggio;

Struttura dell'edificio:

Il sito della sede centrale è circondato da una protezione perimetrale con cancelli d'accesso che sono sorvegliati durante le ore di attività e chiusi a fine giornata lavorativa. Inoltre l'edificio è circondato su tutti i lati da fari illuminanti nel periodo notturno. Dispone inoltre di fari anche per l'illuminazione di lati o cortili interni. La sede non è difesa nelle porte d'accesso e nelle finestrature con vetri antisfondamento o inferriate. E' dotata di impianto allarme collegato con l'Istituto di vigilanza individuato dall'Ente Locale proprietario. L'edificio, costruito negli anni '80, si presenta efficiente sia per quanto concerne gli impianti tecnologici che relativamente alla struttura architettonica interna.

I locali dove vengono trattati dati personali, sia per mezzo di documenti cartacei che attraverso applicazioni ed archivi informatici, sono situati all'interno dell'area separata dedicata agli uffici il cui accesso è sempre presidiato durante il normale svolgimento dell'attività lavorativa.

Misure di sicurezza (TU 81/2008)

Il sistema antincendio è costituito da estintori manuali a polvere ed anidride carbonica omologati. E' garantita la manutenzione con controllo d'efficienza semestrale da parte di una società specializzata e si provvede ad assicurare la continuità nell'addestramento di personale preposto sull'uso degli estintori stessi.

È stato predisposto un piano d'evacuazione. Sono ubicati nei punti necessari e visibili al pubblico le procedure scritte da seguire in caso d'emergenza ed è funzionante l'impianto d'illuminazione d'emergenza nei locali d'accesso al pubblico.

Alimentazione elettrica e sistemi di continuità

L'impianto elettrico è a norma come anche la cablatura della rete informatica. Esiste la dichiarazione di conformità firmata dall'installatore. È presente l' impianto di messa a terra che è sottoposto a regolare manutenzione.

È presente per le postazioni di lavoro e il server un sistema d'alimentazione, specifico, dedicato, separato dagli altri contesti utilizzatori e con potenza adeguata, che soddisfa la necessaria continuità elettrica di funzionamento.

3. RESPONSABILITA'

I responsabili, gli incaricati del trattamento e i manutentori del sistema sono individuati con apposito provvedimento che specifica finalità e modalità del trattamento autorizzate nonché tipologie di comunicazione e diffusione ammesse (Allegato C).

Titolare del trattamento

Titolare del trattamento è l'IISS "Leonardo da Vinci" con sede centrale in via Padre Angelo Centrullo s.n., a Cassano delle Murge (BA), nella veste del suo rappresentante legale pro-tempore, il Dirigente Scolastico.

Il Dirigente Scolastico in qualità di titolare del trattamento dei dati

- è responsabile dell'analisi e della valutazione dei rischi ai fini dell'adozione di misure di sicurezza, sia idonee che minime;
- procede alla predisposizione delle misure idonee ritenute indispensabili nella struttura, valuta la congruità tecnico-economica delle misure proposte e quindi disporre l'adozione delle stesse;
- individua il/i responsabile/i del trattamento e con apposito incarico ne stabilisce le responsabilità in merito al rispetto degli adempimenti e delle prescrizioni stabiliti sulla base del D.Lgs196/03;
- si avvale della collaborazione del D.S.G.A. e dei responsabili dei diversi settori per la definizione della modulistica e delle procedure.

Responsabile del trattamento

Al responsabile del trattamento sono attribuiti incarichi di ordine organizzativo e direttivo, ed egli provvede a:

- individuare e designare per iscritto gli incaricati del trattamento che operano sotto la sua diretta autorità indicando puntualmente l'ambito del trattamento consentito;
- impartire loro specifiche istruzioni scritte relative alle modalità di trattamento ammesse;
- coadiuvare il Titolare nell'organizzare la formazione per gli incaricati;

- procedere alle verifiche specificate nell'incarico.

E' individuato quale Responsabile del trattamento dei dati comuni e sensibili: il Direttore SGA, Rag. Vito Antonio ATTOLLINO.

Amministratore di Sistema

Il Titolare del trattamento conferisce l'incarico di Amministratore di Sistema al soggetto incaricato di sovrintendere alle Risorse Informatiche dell'Istituto secondo quanto stabilito nel Disciplinare interno (Allegato B) per l'utilizzo delle strumentazioni informatiche, della rete internet e della posta elettronica.

L'Amministratore di Sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, ha facoltà di accedere, previa autorizzazione dell'utente interessato, anche da remoto, al personal computer di ciascun dipendente. E' individuato quale amministratore di sistema: il prof. Leonardo CAMPANALE.

Incaricati del trattamento

L'assegnazione del personale docente e ATA alla specifica unità operativa, per la quale è individuato con atto formale, comporta l'automatico incarico al trattamento autorizzato per iscritto agli addetti all'unità medesima e la consegna, a cura del Responsabile del Trattamento, delle specifiche istruzioni scritte relative alle modalità di trattamento ammesse.

Per il personale amministrativo la designazione per iscritto riguarda un singolo incaricato e con essa si individua l'ambito del trattamento a questi consentito.

Tali incarichi sono assegnati a partire dal 1° settembre, data di inizio del nuovo anno scolastico che coincide con le assegnazioni di sede del personale. Al presente documento è allegato l'elenco dei provvedimenti adottati con i relativi estremi (*Allegato C*).

Sia per i trattamenti effettuati con strumenti elettronici, che per quelli che avvengono senza l'ausilio di tali strumenti, l'autorizzazione al trattamento è soggetta ad aggiornamento periodico e comunque almeno annuale, quando viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione riguardo l'ambito di trattamento consentito sia ai singoli incaricati che agli addetti alla manutenzione e gestione degli strumenti elettronici

4. DATI E BANCHE DATI

Al fine di elaborare l'elenco dei trattamenti dei dati, posti in essere dal Titolare:

- sono precisate le finalità del trattamento;
- sono individuati i tipi di dati personali trattati, in base alla loro natura (comuni, giudiziari o sensibili ed alla categoria di soggetti cui essi si riferiscono (alunni, personale dipendente, fornitori, esperti esterni, consulenti e collaboratori)
- sono definite le operazioni di trattamento dei dati effettuate;
- sono descritte le aree, i locali e gli strumenti con i quali si effettuano i trattamenti.

Finalità del trattamento

Al fine di perseguire le finalità istituzionali, l'IISS "Leonardo da Vinci" effettua operazioni di trattamento di dati personali (sia comuni che sensibili o giudiziari) di studenti e dei loro genitori, personale dipendente, fornitori, esperti esterni, consulenti collaboratori con le seguenti finalità:

a. la selezione e il reclutamento del personale a tempo determinato, nonché l'instaurazione, la gestione e la cessazione del rapporto di lavoro;
b. la frequenza dei corsi di studio;
c. l'espletamento delle attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione ed orientamento, di scrutini ed esami;
d. l'attivazione degli organismi collegiali e delle commissioni istituzionali previsti dall'ordinamento scolastico;
e. l'acquisizione di beni, servizi e opere;
f. la difesa in giudizio del Ministero dell'istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro e amministrative, nonché quelle connesse alla gestione degli affari penali e civili;
g. le attività connesse alla instaurazione di contenzioso (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'autorità giudiziaria, etc.) con gli alunni e con le famiglie, e tutte le attività relative alla difesa in giudizio delle istituzioni scolastiche;
h. gli adempimenti relativi alla pubblicazione sul sito web dell'Istituzione scolastica: http://www.liceocassano.gov.it/ di informazioni alla luce della recente riforma normativa in materia di trasparenza delle pubbliche amministrazioni (D.Lg. n.150/2009 per la cui disciplina è intervenuto di recente il Garante della Privacy con Deliberazione n. 088 del 2/3/2011.

Tipologie di dati trattati

L'IISS "Leonardo da Vinci" con salvezza della possibilità di procedere a successive integrazioni e/o correzioni, tratta *i dati personali di natura comune o sensibile* 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 e giudiziari di cui all'art.4, comma 1, lett. d) del d.lgs. n.196 del 2003 così come descritti nelle schede allegate al D.M. 305 del 7.12.'06 e relativi a origine, convinzioni religiose, filosofiche, politiche e sindacali, stato di salute e vita sessuale.
d. Dati inerenti al livello di istruzione e culturale nonché relativi all'esito di scrutini, esami, piani educativi individualizzati differenziati;
e. Dati inerenti alle condizioni economiche e l'adempimento degli obblighi tributari;
f. 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;
g. 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;
h. Dati inerenti la fornitura e le modalità di pagamento riguardo ad attività professionale a fini formativi;
i. Dati contabili e fiscali;

j. Dati inerenti alla titolarità di diritti, il possesso o la detenzione di beni mobili registrati, mobili o immobili;
k. Dati detenuti in applicazione di disposizioni di origine nazionale o comunitaria, atti o provvedimenti amministrativi, fonti contrattuali.

I dati trattati da questa amministrazione sono noti all'istituzione scolastica, in ragione della produzione di atti e/o dichiarazioni raccolti per iniziativa degli interessati a fruire direttamente, o a beneficio dei minori sottoposti alla potestà ex art. 316 c.c., dei servizi formativi o previa richiesta dell'Ufficio presso i medesimi ovvero presso altri soggetti pubblici e privati in particolare attraverso:

- 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;
- pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

I dati sono accolti e conservati su supporti cartacei e/o informatici e organizzati nelle seguenti banche dati:

- banca dati alunni;
- banca dati personale direttivo, insegnante e ATA a tempo indeterminato e determinato;
- banca dati fornitori (beni e servizi);
- banca dati – contabilità;
- banca dati – retribuzioni;
- banca dati – protocollo.

per ognuna delle quali è predisposta una scheda di processo allegata al presente documento (***Allegato A***). I documenti e le banche dati settoriali allocate nelle varie postazioni di lavoro ricadono per le operazioni di salvataggio, condivisione e comunicazione significativa sotto la responsabilità dei diversi incaricati. Il sistema di abilitazioni dispone l'utilizzo delle informazioni ai soli utilizzatori cui ricade la competenza.

Operazioni di trattamento dei dati effettuate

Sono considerate operazioni di trattamento dei dati quelle di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione dei dati stessi oltre ad interconnessione e raffronti con altro titolare anche effettuate mediante strumenti elettronici.

Delle operazioni di trattamento sono incaricati gli operatori individuati annualmente con apposita nomina che contestualmente precisa le operazioni autorizzate in relazione alle banche dati e alle modalità di trattamento (informatizzato e non).

Aree, locali e archivi ove risiedono i dati e strumenti con i quali si effettuano i trattamenti
Il trattamento dei dati è effettuato nei seguenti locali:

- Ufficio Protocollo, del Personale Docente e Didattica;
- Ufficio Dirigente Scolastico;
- Ufficio del Direttore S.G.A.

<u>Archiviazione cartacea</u>

I documenti sono conservati nei seguenti locali:

1. Archivio storico situato in locale sotterraneo
2. Ufficio del Dirigente scolastico (computers, armadi e armadi blindati);
3. Ufficio del DSGA (computer, armadi e armadi blindati)

4. Ufficio della Didattica, del Personale e del Protocollo nell'archivio corrente (schedari, armadi, computer);

Gli uffici possono essere chiusi a chiave.

Gli armadi per la custodia e l'archiviazione di atti, documenti e supporti, con particolare riferimento a quelli contenenti dati sensibili o giudiziari sono adeguati a garantire la necessaria sicurezza ai dati personali contenuti negli atti, documenti e supporti ivi conservati in quanto muniti di apposite serrature e chiavi. È presente una cassaforte destinata anche al ricovero dei supporti contenenti le copie di sicurezza delle banche dati informatiche. Essa è ubicata al piano terra nell'Ufficio del Dirigente Scolastico, locale diverso da quello del server.

Strumentazioni informatiche

La situazione attuale delle attrezzature informatiche è la seguente:

Locale	Numero postazioni	Trattamenti effettuati
Ufficio Protocollo	1	Dati personali di natura comune, sensibile e giudiziaria
Ufficio Personale	2	Dati personali di natura comune, sensibile e giudiziaria
Ufficio Didattica	2	Dati personali di natura comune, sensibile e giudiziaria
Totale Ufficio Protocollo e Didattica, Personale	**5**	
Dirigente	1	Dati personali di natura comune, sensibile e giudiziaria
Totale Ufficio del Dirigente	**1**	
Ufficio del Direttore SGA	**1**	Dati personali di natura comune, sensibile e giudiziaria
Server	**1**	Dati personali di natura comune, sensibile e giudiziaria
Totale Attrezzature informatiche	**8**	

La rete LAN di Istituto è realizzata con cablaggio strutturato certificato in cat. 5e. La rete degli uffici è isolata fisicamente e logicamente da quella destinata ai laboratori. La rete LAN dispone di un firewall hardware perimetrale che filtra la connessione internet ed applica una doppia NAT dell'indirizzo IP pubblico. La connessione internet destinata alla didattica è separata da quella ad uso degli uffici. La rete informatica destinata ad usi didattici è anche dotata di una connessione wireless protetta con crittografia WPA2 PSK.

Il sistema informativo è basato su architettura client – server. Le banche dati sono centralizzate ed ospitate su un elaboratore centrale che ha la funzione di file server e database server oltre che di controller di dominio primario basato su Active Directory in modo da attuare il maggior grado di tutela e salvaguardia delle stesse.

Il server è ubicato nell'ufficio del DSGA. Il locale è normalmente presidiato dal personale amministrativo e soggetto a regolare chiusura.

Il server divide lo spazio con documenti cartacei a sufficiente distanza di sicurezza.

Programmi applicativi

Sono in dotazione alla scuola software ARGO per la gestione delle aree degli alunni, bilancio, biblioteca, fisco, inventario, magazzino, personale, protocollo ed emolumenti; il Software Microsoft Office Edizione Prof. 2007 con applicativi Word, Excel, Outlook, Power Point, Access, Publisher.

Tutti i programmi software applicativi sono coperti da contratto di manutenzione (migliorativa, correttiva) e assistenza tecnica.

Sistema di videosorveglianza

La sede centrale dell'IISS dispone di un sistema di videosorveglianza che rileva le immagini attraverso alcune telecamere che sono installate presso i laboratori e nei corridoi dell'istituto.

A tal proposito si ricorda che, in ottemperanza al D.Lgs 196/2003, "l'installazione di sistemi di videosorveglianza presso istituti scolastici deve garantire "il diritto dello studente alla riservatezza" (art. 2, comma 2, d.P.R. n. 249/1998) e tenere conto della delicatezza dell'eventuale trattamento di dati relativi a minori.

A tal fine, se può risultare ammissibile il loro utilizzo in casi di stretta indispensabilità (ad esempio, a causa del protrarsi di atti vandalici), gli stessi devono essere circoscritti alle sole aree interessate ed attivati negli orari di chiusura degli istituti, regolando rigorosamente l'eventuale accesso ai dati.

Restano di competenza dell'autorità giudiziaria o di polizia le iniziative intraprese a fini di tutela dell'ordine pubblico o di individuazione di autori di atti criminali (per es. spacciatori di stupefacenti, adescatori, ecc.)."

Pertanto sono state messe in atto le seguenti regole in relazione al sistema di videosorveglianza:

- In ogni area video-sorvegliata e sulla porta di ingresso è stato apposto un cartello ben visibile che informa i visitatori che la zona in cui transitano è una zona video-sorvegliata o videoregistrata;
- Tale informativa contiene gli elementi di informazione previsti dalla legge ed ha un formato e un posizionamento tale da essere chiaramente visibile; in particolare nell'informativa si fa riferimento agli elementi previsti dal Codice (art. 13 del D.Lgs. 196/2003), utilizzando il modello semplificato di informativa "minima" individuato dal Garante nel Provvedimento del 29 aprile 2004, riportando quindi:
  - Il titolare dei dati
  - Le motivazioni per le quali sono rilevate o registrate le immagini: sicurezza dei beni e delle persone.
  - Una immagine stilizzata di una telecamera
  - Riferimenti opportuni all'art. 13 del D.Lgs. 196/2003
- Le persone fisiche, incaricate del trattamento, autorizzate a utilizzare gli impianti e, nei casi in cui è indispensabile per gli scopi perseguiti, a visionare le registrazioni sono le seguenti: prof. Elio RACANO
- La registrazione dei dati è effettuata con sistema automatico ed è limitata a poche ore, o al massimo, alle ventiquattro/quarantotto ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività, chiusura dell'azienda ecc;
- Un eventuale allungamento dei tempi di conservazione deve essere valutato come eccezionale e comunque in relazione alla necessità derivante da un evento già accaduto o realmente incombente, oppure alla necessità di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria di polizia giudiziaria in relazione ad una attività investigativa in corso;
- Il sistema impiegato è programmato in modo da operare al momento prefissato la cancellazione automatica da ogni supporto, mediante sovraregistrazione, e con modalità tali da rendere non riutilizzabili i dati sovrascritti.

5. CRITERI PER L'INDIVIDUAZIONE E LA VALUTAZIONE DEI RISCHI

Criteri per l'individuazione dei rischi

Per garantire la disponibilità, l'integrità, l'autenticità e la riservatezza delle informazioni, gli articoli da 33 a 36 del Testo Unico in materia di Trattamento dei dati personali di cui al D.Lgs.

30 giugno 2003 n. 196 prevedono l'obbligo di adottare misure minime di sicurezza, ai sensi dell'allegato B del disciplinare tecnico del Testo Unico, che possono essere individuate sulle base di tre grandi categorie di rischi:

- rischi connessi ad eventi relativi al contesto fisico ambientale;
- rischi connessi al mancato rispetto da parte degli operatori degli adempimenti e delle prescrizioni statuite sulla base del disposto Testo Unico in materia di trattamento di dati personali;
- rischi propri del sistema informatico utilizzato dall'Istituto Scolastico.

L'analisi dei possibili rischi è stata, pertanto suddivisa in tre settori di rischio nettamente differenti e separati per tipologia e materia.

A. Eventi relativi al contesto fisico – ambientale

In questo settore sono stati identificati e valutati i rischi legati ad eventi incontrollabili o astrattamente preventivabili di origine fortuita, dolosa o colposa (es. legati alla eventualità che persone non autorizzate possano accedere nei locali) e sono riferiti al luogo dove gli strumenti sono ubicati e quindi agli archivi esistenti negli uffici, agli elaboratori in rete ed ai server ivi ubicati.

Fonti di rischio	*Rischio*
1. Accessi non autorizzati a locali ad accesso ristretto	– Dispersione, perdita o alterazione, anche irreversibile, di dati; – visione abusiva di dati, furto di documenti, uso non autorizzato dei dati; – manomissione di programmi e di elaboratori; – impossibilità temporanea di accesso ai dati e di utilizzo dei programmi.
2. Asportazione e furto di strumenti contenenti dati	– Dispersione e perdita di dati, di programmi e di elaboratori; – accesso altrui non autorizzato
3. Movimenti tellurici, scariche atmosferiche, incendi, allagamenti, eventi distruttivi dolosi, accidentali o dovuti ad incuria o vandalismo	– Perdita di dati, dei programmi e degli elaboratori
4. Guasti a impianto elettrico, gruppo di continuità, climatizzazione, etc.	– Perdita o alterazione, anche irreversibile, di dati; – manomissione dei programmi e degli elaboratori; – impossibilità temporanea di accesso ai dati e di utilizzo dei programmi

B. Comportamento degli operatori

In questo primo settore sono stati identificati e valutati i rischi legati all'attività delle persone (docenti ed ATA) incaricate del trattamento dei dati.

Fonti di rischio	*Rischio*
5. Mancato rispetto del divieto di accesso agli archivi fisici o informatizzati non autorizzati	– Sottrazione / presa visione / copia abusiva di informazioni e dati;
6. Mancata custodia, anche temporanea, dei documenti estratti dall'archivio	– potenziale diffusione di dati anche quando non intenzionale (es. cestinare un semplice documento cartaceo senza provvedere alla sua distruzione);

7. Mancata custodia, anche temporanea, della propria postazione informatica, una volta resa accessibile con le proprie credenziali di autenticazione	– distruzione / alterazione di dati.
8. Mancata chiusura dei contenitori, degli armadi e dei locali adibiti ad archivio	
9. Mancata distruzione dei supporti raggiunta la finalità	
10. Mancata conservazione o restituzione dei documenti cartacei	– Cancellazione anche accidentale di dati e conseguente loro perdita; – alterazione di dati; – trattamento illegittimo di dati per loro comunicazione a soggetti non autorizzati; – trattamento non conforme alle finalità della raccolta; – comunicazioni/diffusione di dati personali non previste preventivamente dalla legge
11. Comportamenti imprevisti, imprudenti o negligenti, errori materiali dei soggetti legittimati al trattamento dei dati	
12. Comportamenti dolosi dei soggetti legittimati	

C. Eventi relativi agli strumenti

In questo settore sono stati identificati e valutati i rischi legati alle infrastrutture tecnologiche (risorse hardware e software) e il rischio di intrusione nelle reti di comunicazione durante la normale attività del sistema informatico. Tali rischi sono collegati a :

- tasso di obsolescenza delle apparecchiature,
- modalità di esecuzione delle copie di sicurezza,
- funzionalità di accesso,
- quote disco condivise in lettura,
- rete di comunicazione accessibile al pubblico,
- utilizzo di periferiche di input.

Fonti di rischio	*Rischio*
1. Azione di virus informatici con conseguente danno HW e/o SW	– Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori.
2. Alterazione HW e SW a causa 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.
3. Alterazione o distruzione di dati a causa di sabotaggio	
4. Malfunzionamento, indisponibilità o degrado degli strumenti HW	
5. Malfunzionamento SW	
6. Guasto Tecnologico	
7. Accessi esterni non autorizzati	– Presa visione, copia abusiva, sottrazione di dati; – perdita o alterazione, anche irreversibile, di dati; – uso non autorizzato di applicativi; – manomissione di programmi e di elaboratori; – impossibilità temporanea di accesso ai dati e di utilizzo dei programmi.
8. Perdita delle copie di back-up	– Presa visione, copia abusiva, – perdita, anche irreversibile, di dati;
9. Perdita o riutilizzo non autorizzato di supporti magnetici	

10. Intercettazione delle trasmissioni di dati	– Diffusione di dati.

Criteri per la valutazione dei rischi

Una volta individuati i rischi, per procedere alla loro valutazione è necessaria una indicizzazione delle possibili perdite tenendo in considerazione due fattori:

- probabilità (**P**) di accadimento, che riguarda la frequenza riscontrata o riscontrabile:

Probabilità

1	Non sono noti episodi.	IMPROBABILE
2	Sono noti rarissimi episodi.	POCO PROBABILE
3	Noto qualche episodio in cui la mancanza rilevata ha fatto seguito a un danno.	PROBABILE
4	Si sono verificati danni per la stessa mancanza rilevata in situazioni simili.	ALTAMENTE PROBABILE

- magnitudo (**M**) delle conseguenze nel caso l'evento si verifichi. In effetti la valutazione del rischio nel trattamento del dato deve tener conto sia della sua importanza che del danno legato al diritto che verrebbe ad essere leso.

Dobbiamo quindi distinguere diverse tipologie di dati
- dati conoscibili da chiunque,
- dati accessibili ai sensi della legge 241/90,
- dati sensibili e giudiziari

a cui corrisponde diverso grado di rischio intrinseco connesso alla loro perdita, alterazione, comunicazione o diffusione perché:
- idonei a rivelare informazioni di carattere sensibile o giudiziario dei soggetti interessati, che sono quindi accomunati dall'elevato grado di pericolosità per la privacy dei soggetti interessati,
- costituiscono una importante risorsa, funzionale e tecnologica, per il Titolare, in relazione ai danni che conseguirebbero da una eventuale loro perdita.

Ne conseguono i seguenti criteri:

			Magnitudo
1	Perdita dei dati	diritto alla protezione	BASSA
2	Alterazione dei dati	diritto all'identità personale	MEDIA
3	Trattamento illecito/diffusione/comunicazione di dati personali	diritto alla riservatezza	MEDIO - ALTA

4	Trattamento illecito/diffusione/comunicazione di dati sensibili	diritto alla riservatezza	ALTA

Il Rischio (R) è la risultante della probabilità e della gravità di un evento: **R = P x M;** dando a **P** e a **M** un valore fra 1 e 4, si ottiene un valore **R** compreso fra 1 e 16.

6. INDIVIDUAZIONE E VALUTAZIONE DEI RISCHI

Si è proceduto all'individuazione dei rischi utilizzando le apposite matrici, in cui sono riportati i singoli fattori di rischio divisi sulla base dei possibili accadimenti relativi a:

- Contesto fisico – ambientale (Tavola 1);
- Comportamento degli operatori (Tavola 2);
- Sistema informatico utilizzato dall'Istituto scolastico (Tavola 3).

Nell'analisi dei rischi, questi sono stati valutati astrattamente, cioè a prescindere dalle misure che sono state già adottate, per facilitare sia la verifica dell'idoneità e l'efficacia delle misure stesse che la valutazione degli interventi adeguativi necessari. Le tavole di valutazione del rischio riportano: fonte di rischio, magnitudo del rischio, probabilità del rischio, rischio calcolato.

7. MISURE DI PROTEZIONE NECESSARIE IN REAZIONE AL CONTESTO DESCRITTO

Dopo aver analizzato e valutato i fattori di rischio di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, sono state individuate le misure di prevenzione e protezione più idonee a:

- eliminare il rischio,
- prevenire il rischio per diminuire la probabilità di accadimento;
- contenere l'impatto di un evento dannoso e diminuire la gravità degli effetti causati eventualmente dall'accadimento ;
- trasferire le conseguenze patrimoniali dell'evento (es. stipula contratto di assicurazione).

Nell'individuazione di tali misure sono presi in considerazione i seguenti aspetti:

- leggi, raccomandazioni e normative;
- sicurezza fisica e logica;
- definizione di ruoli, incarichi, procedure e formazione del personale;
- costi in relazione agli obiettivi e alle risorse disponibili.

Le matrici (***Tavole 1, 2, 3***), in cui sono riportati i singoli fattori di rischio registrano anche:

- le misure ritenute idonee per eliminarli, prevenirli, contenere o trasferire il rischio,
- le misure in essere al momento in cui viene effettuata la valutazione dei rischi,
- le misure che devono essere adottate e il termine entro cui le stesse vanno assunte.

Misure fisiche

	Rischio	*Misure di protezione*	
01	Sottrazione / presa visione / copia abusiva di informazioni e dati conseguente a - accessi non autorizzati a locali ad accesso ristretto; - asportazione e furto di strumenti contenenti dati.	Vigilanza della sede	- Chiusura a chiave locali - Sistemi di allarme - Cartelli segnaletici di divieto di accesso
		Custodia e archiviazione di atti, documenti e supporti	- Chiusura a chiave locali e armadi - Procedura gestione chiavi - Autenticazione accessi - Custodia in armadi blindati
02	Perdita di dati dovuta a - movimenti tellurici, scariche atmosferiche, incendi, allagamenti, eventi distruttivi dolosi, accidentali o dovuti ad incuria o vandalismo - guasti a impianto elettrico, gruppo di continuità, climatizzazione, etc.	Adeguamento e manutenzione strutture ed impianti	- Impianto elettrico a norma - Sistemi di protezione antincendio - Impianto di messa a terra - PC sollevati da terra per proteggerli in caso di allagamento

Alle misure individuate devono accompagnarsi quelle di natura organizzativa che riguardano:

- l'assegnazione di incarichi, autorizzazioni e compiti al personale dipendente;
- le istruzioni operative agli incaricati per il servizio di sorveglianza, la custodia e l'archiviazione di atti, documenti e supporti, le modalità di accesso, il controllo delle presenze di personale e alunni;
- la definizione di procedure per i controlli fisici all'accesso, la gestione delle chiavi, il carico/scarico di documenti, la manutenzione degli impianti e dei locali.

Particolare attenzione è prestata per gli archivi e i documenti relativi a dati sensibili e giudiziari affinché ai dati non possano accedere persone prive di autorizzazione.

Misure organizzative

Individuati e valutate tutte le fonti di rischio e i rischi annessi, sulla base dell'analisi del flusso dei dati e dei soggetti ai quali vengono comunicati, sono stati determinati i seguenti provvedimenti :

- individuazione dei responsabili e degli incaricati al trattamento (*Allegato C*);
- istruzioni operative per il personale con misure graduate per classi di dati (*Allegato B*).

	Rischio	**Misure di protezione**	
01	Perdita o alterazione di dati dovuta a - mancata conservazione o restituzione dei documenti cartacei; - ad errori materiali o a comportamenti imprudenti o negligenti;	Istruzioni operative Controlli periodici	- Istruzioni organizzative e tecniche;

02	Diffusione di dati causata da - mancata custodia dei documenti o della propria postazione, - mancata chiusura dei contenitori, degli armadi e dei locali adibiti ad archivio, - mancata distruzione dei supporti raggiunta la finalità		- Istruzioni organizzative e tecniche sui comportamenti da tenere; - sorveglianza sulla distruzione dei supporti rimovibili; - presenza in segreteria di appositi distruggi documenti cartacei;
03	Trattamento non conforme o illegittimo di dati e loro comunicazione o diffusione a soggetti non autorizzati	Assegnazione incarichi Istruzioni operative Controlli periodici	- Adozione di procedure riguardo a soggetti e modalità con cui i dati possono essere comunicati dalla segreteria scolastica verso l'esterno
04	Sottrazione / presa visione / copia abusiva di informazioni e dati conseguente al mancato rispetto del divieto di accesso agli archivi fisici o informatizzati non autorizzati.	Log file Ingresso controllato	- Organizzazione servizio di sorveglianza - Credenziali di accesso - Consultazioni registrate - Controllo fotocopiatura (Fotocopiatrice con chiave e registrazione numero copie)

Si ritiene infine che solo un'adeguata conoscenza del disposto normativo può realmente e proficuamente garantire l'osservanza del medesimo ed, in definitiva, abbattere i rischi connessi a questo settore che è sicuramente il più rilevante e quindi quello a cui vanno dedicate le maggiori attenzioni per garantire un trattamento dei dati conforme alle prescrizioni legislative.

Misure logiche

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), è stato predisposto uno specifico *Disciplinare tecnico* con le norme di comportamento da tenere (*Allegato B*) per evitare:

- i rischi di intrusione,
- la diffusione illegittima di dati,
- l'accesso abusivo.

	Rischio	Misure di protezione	
01	Perdita o alterazione di dati / applicativi dovuta a - azione di virus informatici con conseguente danno HW e/o SW; - alterazione HW e SW a causa di sabotaggio; - malfunzionamento, indisponibilità o degrado degli strumenti HW o SW; - perdita delle copie di back-up; - disponibilità di periferiche di input	Disciplinare tecnico Contratti di assistenza tecnica applicativa e sistemistica Servizi di manutenzione correttiva e straordinaria dei programmi	- Firewall antintrusione come modulo software ed appliance hardware; - Intrusion Prevention ed Intrusion detection systems - Data Loss Prevention - Servizio di filtraggio antivirus e antispamming per il controllo dei messaggi e degli allegati di posta elettronica, - Controllo delle pagine Internet in ordine a cookies, activex, java; - Controllo antivirus in automatico di ogni file scaricato dalla rete o letto da supporti esterni di memorizzazione; - Aggiornamento automatico con frequenza almeno giornaliera dell'antivirus; - Back-up giornaliero della base dei dati dei programmi applicativi - Back-up periodico degli archivi - Deposito delle copie di sicurezza in armadi dislocati presso l'Ufficio del Direttore SGA
02	Diffusione di dati causata da intercettazione delle trasmissioni		- Ricorso a tecniche di crittografia per assicurare la riservatezza; - ricorso a tecniche in grado di assicurare la non modificabilità delle informazioni durante la trasmissione; - meccanismi di notifica di ricezione per verificare il non ripudio da parte del destinatario; - firma digitale per assicurare da parte del mittente requisiti di autenticazione, utili anche per il non ripudio.
03	Sottrazione / presa visione / copia abusiva di informazioni e dati conseguente ad accessi non autorizzati.		- Adozione di un sistema di credenziali di autorizzazione tramite profili utente e password complesse alfanumeriche con numero di caratteri non inferiori ad otto. - Separazione sistema server di dati ed applicazioni dell'Istituto dal gateway internet; - Controllo e registrazione accessi

L'accesso al sistema informatico è consentito alle sole persone autorizzate, poiché è protetto da un sistema di credenziali di autorizzazione basato su Active Directory ed è previsto un registro di controllo delle presenze. È utilizzato un sistema di sicurezza internet che comprende un firewall software un antivirus, IPS, IDS e DLP, in grado di riconoscere virus polimorfici, prevenire ed identificare intrusioni, controllare le attività sul Personal Computer, i messaggi e gli allegati di posta elettronica, le pagine Internet in ordine a cookies, controlli ActiveX e Java. Il sistema ha una frequenza di aggiornamento almeno giornaliera. La posta elettronica istituzionale è gestita su tutte le postazioni sotto forma di webmail e su una postazione della segreteria, che funge da archivio, è attivato un client di posta elettronica. Viene effettuato un backup periodico dei file di posta elettronica. L'antivirus controlla in automatico ogni file scaricato dalla rete o letto da supporti esterni di memorizzazione ed è pianificato un controllo approfondito periodico di tutti i file presenti nel sistema. Il personale ha ricevuto le necessarie istruzioni al fine di evitare l'introduzione di virus informatici nella rete. L'accesso ad Internet è

consentito utilizzando la rete LAN mediante un unico punto (router ADSL) separato e distinto dal sistema server di dati e di applicazioni dell'Istituto.

Misure di sicurezza suppletive relative al trattamento di particolari dati sensibili

In caso di trattamento di dati sensibili o giudiziari (punto 19.8 del D.Lgs. n. 196/2003) ed in particolare per i dati personali idonei a rivelare lo stato di salute, devono essere adottati particolari accorgimenti:

1. la custodia / archiviazione di tali dati separatamente dagli altri dati personali dell'interessato;
2. l'accesso, per la consultazione e/o modificazione, condizionato dal rispetto della procedura di identificazione per cui:

    a. l'incaricato deve essere precisamente individuato ed autenticato;
    b. l'incaricato può trattare i dati sensibili solo con un appropriato profilo di autorizzazione;
    c. l'incaricato deve essere in possesso della chiave di accesso.

I dati sensibili debbono essere nettamente separati e gestiti autonomamente ed indipendentemente da ogni incaricato unicamente in base al proprio profilo di autorizzazione e per quel che attiene i dati personali degli alunni riportati sul registri didattici va prevista apposita procedura per la loro raccolta e custodia;

3. la trasmissione dei dati deve avvenire in maniera crittografata;

Programma delle misure

Il programma delle misure di sicurezza adottate o da adottare per ogni categoria di rischi è sistematicamente aggiornato nell'ottica di un miglioramento continuo del Sistema Sicurezza dell'Istituto Scolastico con cadenza annuale e in tutte le occasioni in cui si riscontri necessità di intervento o non conformità (tecniche o normative).

Il criterio adottato dall'Istituto per stabilire uno scadenzario degli interventi considera il tempo, espresso in mesi, in funzione inversa all'indice **R** di gravità:

R = 16 intervento entro 01 mesi e verifica entro 10 giorni;
R = 12 intervento entro 04 mesi e verifica entro 20 giorni;
R = 08 intervento entro 08 mesi e verifica entro 30 giorni;
R = 04 intervento entro 12 mesi e verifica entro 40 giorni
R = 01 intervento entro 16 mesi e verifica entro 60 giorni.

Il programma delle misure di protezione necessarie per il trattamento dei rischi analizzati e valutati è riportato nelle tavole di valutazione dei rischi assieme alla definizione dei tempi previsti per la loro adozione.

Affidamento dei dati a soggetti esterni

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 per iscritto al terzo destinatario. Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come responsabile del trattamento dei dati, mediante apposita lettera scritta.

8. FORMAZIONE DEL PERSONALE

La previsione di interventi formativi degli incaricati del trattamento rientra tra gli aspetti più importanti del presente documento.

In effetti, una gestione impropria da parte del personale ATA chiamato alla gestione dei dati personali nonché del corpo insegnante per quel che attiene il trattamento dei dati degli alunni effettuato con i registri di classe, la mancanza di chiare direttive esplicative e l'assenza di strumenti di controllo di facile e rapida applicazione costituiscono le cause principali del verificarsi, anche inconsapevole, di danni agli interessati ed in definitiva la causa prioritaria di trattamenti illegittimi e non conformi alle specifiche finalità dell'istituzione scolastica.

Gli interventi formativi sono programmati in modo da avere luogo al verificarsi di una delle seguenti circostanze:

- al momento dell'ingresso in servizio;
- in occasione di un cambiamento di mansioni che implichi modifiche rilevanti rispetto al trattamento di dati personali;
- in occasione della introduzione di nuovi significativi strumenti con conseguenti rilevanti modifiche nel trattamento di dati personali.

Scopo della formazione

Il D. Lgs. 196/2003 impone 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. Di conseguenza l'Istituto prevede interventi formativi degli incaricati del trattamento, finalizzati a renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi e procedure da seguire;
- modalità per mantenersi aggiornati sulle misure di sicurezza adottate dal titolare.

Modalità di formazione degli incaricati del trattamento dei dati personali

Sotto la diretta vigilanza e il coordinamento del Titolare del Trattamento è prevista la predisposizione e l'applicazione di un adeguato e dettagliato piano di formazione del personale che contempla la possibilità di:

- ***Aggiornamento Periodico*** sotto la diretta vigilanza del Titolare del Trattamento con cadenza almeno annuale stabilito in coincidenza con l'obbligo di aggiornamento del Documento Programmatico sulla Sicurezza;

- ***Aggiornamento Specifico,*** tempestivamente effettuato ogni qualvolta l'incaricato sia deputato a trattare nuove banche dati oppure utilizzi nuovi strumenti informatici e/o nuove e diverse procedure mediante un programma individuale che deve essere impartito dal Titolare in relazione alla nuova e specifica attività di trattamento svolta.

Gli interventi formativi possono avvenire:

- mediante la consegna di materiale esplicativo riguardante le norme, gli adempimenti richiesti nonché le misure minime di sicurezza applicate dall'Istituto;
- all'interno dell'Istituto, a cura del responsabile per la sicurezza, del responsabile al trattamento o di altri soggetti esperti nella materia,
- all'esterno dell'istituto, presso soggetti specializzati.

Valutazione dell'efficienza del piano di formazione

Il Titolare del Trattamento dei dati personali, dopo avere dettagliatamente individuato il contenuto del piano di formazione del personale ATA e degli insegnanti, appronta una serie di strumenti di verifica dell'efficienza della formazione impartita per essere certo che essa sia stata realmente recepita dagli incaricati del trattamento e che sia stata funzionale ad un appropriato e sicuro trattamento dei dati personali.

9. RIPRISTINO DEI DATI

Le misure ritenute idonee 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[1] sono:

1. residenza dei dati in una struttura documentale sul server condivisa in rete e non sui dischi dei singoli P.C.;
2. procedure automatiche di backup dei database e dei dati contenuti nel server su supporti adeguati alla quantità di dati che deve essere salvata;
3. copie di backup giornaliere su hard disk per le banche dati gestionali e istruzioni organizzative e tecniche che prevedono il salvataggio con frequenza almeno settimanale per quanto riguarda la gestione documentale;
4. etichettatura ed archiviazione dei supporti utilizzati per il backup dei dati con conservazione delle copie di sicurezza in cassaforte;
5. procedure di recupero immediato dei dati in caso di attacchi;
6. analisi e test di tutti i software in possesso dell'Istituto scolastico di tutti gli hardware nonché tutti gli altri strumenti informatici tecnico-operativi dell'intero sistema informatico scolastico.

Sono salvati anche i sistemi attraverso la copia della configurazione di sistema/rete su hard disk di backup e copie del sistema operativo e degli applicativi presenti nei server, tramite backup su hard disk e CD/DVD affinché siano ripristinabili. Si provvede al rifacimento di tali copie con periodicità dettata dagli interventi di manutenzione e aggiornamento del software di base (sistemi operativi, piattaforme database, ecc.) e dei programmi applicativi.

Per quanto riguarda i documenti cartacei e i supporti diversi da quelli elettronici contenenti dati personali, essi sono fascicolati e depositati:

- **presso l'archivio generale** per quanto riguarda gli atti acquisiti al **Protocollo** degli anni precedenti, i **fascicoli del Personale** Direttivo, Docente ed ATA trasferiti e/o in Pensione, Documenti contabili, emolumenti datati da 5 anni addietro , **Fascicoli degli alunni**, **Registri perenni** amministrativi e didattici, compiti degli alunni degli ultimi 5/6 anni
- **nell'archivio corrente** per quanto riguarda tutti gli atti acquisiti al Protocollo degli ultimi due anni, i fascicoli del Personale Direttivo, Docente e ATA in servizio, Fascicoli degli alunni frequentanti, documenti amministrativi, Contabili ed emolumenti degli ultimi 5/6 anni.

10. ATTIVITA' DI CONTROLLO E VALUTAZIONE

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il responsabile del trattamento e le persone da questo appositamente incaricate provvedono, in modo estemporaneo, anche con verifiche casuali e non annunciate e/o con controlli a campione, a verificare che le misure implementate, sia quelle tecnologiche che quelle organizzative, siano effettivamente applicate e svolgano correttamente le funzionalità per cui sono state adottate.

Tale verifica si sostanzia nelle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento

[1] La legge sul protocollo, superando la norma del codice, richiede che il sistema sia recuperabile in esercizio entro 24 ore.

- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici;
- verificare l'integrità dei dati e delle loro copie di backup;
- verificare la sicurezza delle trasmissioni in rete;
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti;
- verificare il livello di formazione degli incaricati.

Almeno ogni sei mesi, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi. Mediante l'analisi dei log file e adottando strumenti automatici di reportistica e di sintesi, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli incaricati per il loro tramite, è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette. Delle attività di verifica svolte viene redatto apposito verbale, che viene conservato dal Titolare del trattamento. In sede di valutazione il Titolare del trattamento, coadiuvato dal Responsabile del trattamento e dall'Amministratore di sistema, analizza l'efficacia degli strumenti adottati al fine di

- rivedere se necessario l'indice di gravità dei rischi controllando quali danni si sono avuti o quali siano possibili, la frequenza degli accadimenti registrati, le circostanze in cui si sono subiti attacchi;
- individuare le misure che sono risultate non adeguate e che vanno riconsiderate.

Al responsabile del trattamento è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

In merito alle "Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul sito web" adottate dal Garante della privacy con deliberazione n. 088 del 2/3/2011, si precisa che essendo stato recentemente rinnovato il sito web Istituzionale dell'Istituto, si sta provvedendo ad uniformarsi sia alle predette linee guida che a quanto previsto nel "Programma triennale per la trasparenza e l'integrità " come previsto dal D.Lg. n. 150/2009 in materia di trasparenza delle pubbliche amministrazioni.

Il presente documento, redatto il giorno 16 Maggio 2016, è stato assunto al protocollo dell'Istituto in data 16 Maggio 2016 col numero 2842

L'originale del presente documento viene custodito presso l'Amministrazione Scolastica, per essere esibito in caso di controlli.

Il Titolare del trattamento

Dott.ssa Daniela CAPONIO

Istituto di Istruzione Secondaria Superiore
LICEO SCIENTIFICO E CLASSICO STATALE
LEONARDO DA VINCI

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it

Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

TAVOLA 1 - Fonti di rischio collegate al contesto fisico-ambientale

1. Accessi non autorizzati a locali ad accesso ristretto e conseguenti possibilità di furto, sabotaggio, presa visione abusiva atti, furto di documento, uso non autorizzato dei dati.
2. Furto di strumenti informatici contenenti dati.
3. Movimenti tellurici, scariche atmosferiche, incendi, allagamenti, eventi distruttivi dolosi, accidentali o dovuti ad incuria o vandalismo.
4. Guasti a impianto elettrico, gruppo di continuità, climatizzazione, etc.

	Fonte di rischio	M	P	R	Misure Idonee	Misure Adottate	Misure da Adottare ...	... entro
1	Ingresso non controllato	3	2	3x2 = 6	Organizzazione servizio di sorveglianza Sistemi di allarme	Sistema di allarme.		
2	Ingresso non autorizzato	2	2	2x2 = 4	Istruzioni operative per servizio di sorveglianza Controllo presenze personale e alunni	Controllo diretto presenze personale ed alunni secondo precise istruzioni operative per il servizio di sorveglianza		
3	Accesso non autorizzato archivi dati comuni	2	2	2x2 = 4	Assegnazione incarichi Chiusura a chiave locali e armadi Procedura gestione chiavi Cartelli segnaletici di divieto di accesso	Chiusura a chiave Assegnazione incarico	Procedura gestione chiavi Cartelli segnaletici	12 mesi
4	Accesso non autorizzato archivi dati sensibili o giudiziari	4	2	4x2 = 8	Assegnazione incarichi Chiusura a chiave locali e armadi Casseforti Procedura gestione chiavi Procedura carico/scarico documenti Istruzioni operative	Assegnazione incarichi Chiusura a chiave locali e armadi Casseforti Procedura gestione chiavi Procedura carico/scarico documenti Istruzioni operative		
5	Fotocopie abusive	2	2	2x2 = 4	Fotocopiatrice con chiave Registrazione numero copie	Fotocopiatrice con chiave Registrazione numero copie		
6	Furto HW	2	1	2x1 = 2	Chiusura a chiave locali Sistemi di allarme Back-up	Chiusura dei locali a chiave. Inserimento sistema di allarme alla chiusura dei locali. Backup dei dati conservati in locali diversi da quelli dell'istituto.		
7	Furto o copiatura SW	2	1	2x1 = 2	Credenziali di accesso Back-up Log file (solo sul backup dei server)	Adozione di credenziali di accesso individuali . Esecuzione di backup programmati. Adozione di un		

						sistema di registrazione del log degli accessi sul server		
8	Incendio	3	2	3x2 = 6	Sistemi di protezione antincendio Piano di emergenza Back-up	Sistemi di protezione antincendio Piano di emergenza Back-up		
9	Allagamento	2	2	2x2 = 4	PC sollevati da terra Piano di emergenza Back-up	PC sollevati da terra Piano di emergenza Back-up		
10	Scariche atmosferiche	2	2	2x2 = 4	Impianto di messa a terra Regolare manutenzione Back-up	Impianto di messa a terra Regolare manutenzione Back-up		
11	Cedimento strutturale / Terremoto	3	2	3x2 = 6	Costruzione antisismica Piano di emergenza Back-up	Piano di emergenza Back-up		
12	Cortocircuito	1	2	1x2 = 2	Impianto certificato	Impianto certificato		
13	Mancanza di alimentazione elettrica	1	3	1x3 = 3	Gruppo di continuità Back-up	Gruppo di continuità Back-up		

Istituto di Istruzione Secondaria Superiore
LICEO SCIENTIFICO E CLASSICO STATALE
LEONARDO DA VINCI

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it
Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

TAVOLA 2 - Fonti di rischio collegate al comportamento degli operatori

1. Possono venire sottratte o cedute le credenziali di autenticazione con conseguente accesso a dati per cui non esiste autorizzazione;
2. I soggetti legittimati al trattamento dei dati possono mettere in atto comportamenti imprevisti, imprudenti o negligenti o errori materiali che danneggiano i dati o ne consentono la loro comunicazione e/o diffusione;
3. I soggetti legittimati possono mettere in atto comportamenti dolosi per manomettere o acquisire informazioni custodite dall'Istituto.

	Fonte di rischio	M	P	R	Misure Idonee	Misure Adottate	Misure da Adottare...	... entro
1	Assenza del personale incaricato	1	3	1x3 = 3	Gestione risorse umane Formazione	Formazione del personale		
2	Mancato rispetto del divieto di accesso agli archivi fisici o informatizzati non autorizzati e conseguente sottrazione / presa visione abusiva di informazioni e dati	3	1	3x1 = 3	Credenziali di accesso Istruzioni operative Log file	Adozione di un sistema di credenziali di accesso costituito da profili utente protetti da password complesse con obbligo di cambiamento delle stesse ogni 45 giorni. Vengono impartite istruzioni operative circa i rischi connessi all'uso delle postazioni di lavoro. Adozione di un sistema di memorizzazione degli accessi effettuati sul server		
3	Cancellazione di dati e conseguente loro perdita	1	2	1x2 = 2	Credenziali di accesso Back-up Istruzioni operative Log file	Adozione di un sistema di credenziali di accesso costituito da profili utente protetti da password complesse con obbligo di cambiamento delle stesse ogni 45 giorni. Utilizzo di un sistema automatico di backup pianificati giornalieri dei dati presenti su server. Vengono impartite istruzioni operative circa i rischi connessi all'uso delle postazioni di lavoro. Adozione di un sistema di memorizzazione dei log degli accessi effettuati sul server		

4	Alterazione di dati	2	2	2x2 = 4	Credenziali di accesso Back-up Istruzioni operative Log file	Adozione di un sistema di credenziali di accesso costituito da profili utente protetti da password complesse con obbligo di cambiamento delle stesse ogni 45 giorni. Utilizzo di un sistema automatico di backup pianificati giornalieri dei dati presenti su server. Vengono impartite istruzioni operative circa i rischi connessi all'uso delle postazioni di lavoro. Adozione di un sistema di memorizzazione dei log degli accessi effettuati sul server		
4	Comunicazione/diffusione illegale dei dati e dei documenti	3	1	3x1 = 3	Credenziali di accesso Istruzioni operative Controllo fotocopiatura	Adozione di un sistema di credenziali di accesso costituito da profili utente protetti da password complesse con obbligo di cambiamento delle stesse ogni 45 giorni. Vengono impartite istruzioni operative e si effettua un controllo dell'operatività del fotocopiatore tramite la limitazione delle copie agli operatori che dispongono della chiave di accesso e registrazione del numero di fotocopie effettuate.		
5	Mancata custodia, anche temporanea, dei documenti estratti dall'archivio o della postazione informatica quando "accessibile"	3	2	3x2 = 6	Istruzioni operative Verifiche	Istruzioni operative. Verifiche		
6	Mancata custodia, anche temporanea, della propria postazione una volta connessi al sistema con le proprie credenziali di autenticazione	3	2	3x2 = 6	Istruzioni operative Verifiche	Istruzioni operative. Verifiche		
7	Mancata conservazione o restituzione dei documenti cartacei	2	1	2x1 = 2	Istruzioni operative Verifiche	Istruzioni operative. Verifiche		
8	Mancata chiusura dei contenitori, degli armadi e dei locali adibiti ad	3	2	3x2 = 6	Istruzioni operative	Istruzioni operative. Verifiche		

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it
Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

	archivio				Verifiche			
9	Perdita, mancata distruzione o riutilizzo non autorizzato dei supporti raggiunta la finalità	3	2	3x2 = 6	Istruzioni operative Verifiche	Istruzioni operative. Verifiche		
10	Mancata custodia, anche temporanea, dei documenti contenenti dati sensibili o giudiziari estratti dall'archivio	4	2	4x2 = 8	Istruzioni operative Verifiche	Istruzioni operative. Verifiche		
11	Mancata chiusura dei contenitori, degli armadi e dei locali adibiti ad archivio per i documenti contenenti dati sensibili o giudiziari	4	2	4x2 = 8	Istruzioni operative Verifiche	Istruzioni operative. Verifiche		
12	Perdita, mancata distruzione o riutilizzo non autorizzato dei supporti contenenti dati sensibili o giudiziari raggiunta la finalità	4	2	4x2 = 8	Istruzioni operative Verifiche	Istruzioni operative. Verifiche		

TAVOLA 3 - Fonti di rischio collegate al sistema informatico utilizzato dall'Istituto

1. Azione di virus informatici o interventi di sabotaggio con conseguente perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori o impossibilità temporanea di accedere ai dati e di utilizzare i programmi.
2. Malfunzionamento, indisponibilità o degrado degli strumenti HW o SW.
3. Accessi esterni non autorizzati e conseguente presa visione, copia abusiva, sottrazione perdita o alterazione di dati, uso non autorizzato di applicativi o manomissione di programmi e di elaboratori.
4. Intercettazione di informazioni in rete e conseguente diffusione di dati.

	Fonte di rischio	M	P	R	Misure Idonee	Misure Adottate	Misure da Adottare …	… entro
1	Azione di virus informatici con conseguente danno HW e/o SW	4	4	4x4 = 16	Antivirus aggiornato Assistenza Back-up dei programmi applicativi	Utilizzo di un sistema di sicurezza internet dotato di Firewall, IDS, IPS, DLP, antivirus con funzionalità antispyware con aggiornamento automatico pianificato almeno giornaliero. Adozione di un sistema automatico di backup pianificati giornalieri dei dati. Manutenzione periodica dei sistemi e dei programmi applicativi.		
2	Alterazione HW e SW a causa di sabotaggio	3	2	3x2 = 6	Custodia Assistenza Back-up periodico	Custodia dei locali in presenza di personale ed attivazione del sistema di allarme alla chiusura. Assistenza tecnica periodica dei sistemi in dotazione agli uffici. Adozione di un sistema automatico di backup pianificati giornalieri dei dati.		
3	Alterazione o distruzione di dati a causa di sabotaggio	2	2	2x2 = 4	Credenziali di accesso Firewall Back-up periodico Log file	Adozione di un sistema di credenziali di accesso costituito da profili utente protetti da password complesse con obbligo di		

						cambiamento delle stesse ogni 90 giorni. Utilizzo di un sistema di sicurezza internet dotato di Firewall, IDS, IPS, DLP, antivirus con funzionalità antispyware con aggiornamento automatico pianificato almeno giornaliero. Adozione di un sistema automatico di backup periodico pianificato dei dati. Adozione di un sistema di memorizzazione dei log degli accessi effettuati sul server.		
4	Perdita delle copie di back-up	4	1	4x1 = 4	Deposito delle copie di sicurezza in armadi dislocati presso …	Deposito delle copie di sicurezza in cassaforte collocata nell'ufficio del Direttore SGA		
5	Malfunzionamento, indisponibilità o degrado degli strumenti HW	1	2	1x2 = 2	Assistenza Back-up periodico	Esecuzione di interventi di manutenzione periodica programmata delle apparecchiature. Adozione di un sistema automatico di backup periodico pianificato dei dati.		
6	Malfunzionamento SW	1	2	1x2 = 2	Assistenza Back-up periodico	Esecuzione di interventi di manutenzione periodica programmata dei software installati. Adozione di un sistema automatico di backup periodico pianificato dei dati.		
7	Guasto Tecnologico	2	2	2x2 = 4	Manutenzione Back-up periodico	Esecuzione di interventi di manutenzione periodica programmata delle apparecchiature. Adozione di un sistema automatico di backup periodico pianificato dei dati.		
8	Accessi esterni non autorizzati	3	2	3x1=2	Credenziali di accesso	Adozione di un sistema di		

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it
Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

					Firewall Registrazione accessi Back-up periodico	credenziali di accesso costituito da profili utente protetti da password complesse con obbligo di cambiamento delle stesse ogni 45 giorni. Utilizzo di un sistema di sicurezza internet dotato di Firewall, IDS, IPS, DLP, antivirus con funzionalità antispyware con aggiornamento automatico pianificato almeno giornaliero. Adozione di un sistema di memorizzazione dei log degli accessi effettuati sul server. Adozione di un sistema automatico di backup periodico pianificato dei dati.		
9	Intercettazione delle trasmissioni di dati	2	2	2x2 = 4	Crittografia Firma digitale Firewall Formazione personale Rapporti provider	Formazione personale Applicazione di firma digitale crittografata dei documenti. Utilizzo di un sistema di sicurezza internet dotato di Firewall, IDS, IPS, DLP, antivirus con funzionalità antispyware con aggiornamento automatico pianificato almeno giornaliero.	E' prevista l'adozione di un proxy server e di un sistema di content filtering per la connessione internet associato ad un syslog server per il tracciamento completo del traffico internet da tutte le postazioni dell'istituto.	

Istituto di Istruzione Secondaria Superiore
LICEO SCIENTIFICO E CLASSICO STATALE
LEONARDO DA VINCI

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it
Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

Allegato A

Banche dati, finalità e modalità del trattamento autorizzate, tipologie di comunicazione e diffusione ammesse

PERSONALE AMMINISTRATIVO
Banca Dati: ALUNNI

1. Fonte normativa

- T.U. 16.4.1994 n.297, T.U. artt. 309 e 310, D.P.R.22.12.1967 n.1518, D.P.R. 26.1.1999 n.355, Legge 5.2.1992 n.104, D.P.R. 31.8.1999 n.394, D.P.R. 24.7.1977 n.616, L.5.6.1930 n.824, D.P.R. 12.2.1985 n.104, D.P.R. 21.7.1987 n.339
- Regolamento adottato dal MIUR relativo al trattamento dei dati sensibili e giudiziari, pubblicato in G.U. il 15-01-2007

2. Finalità trattamento

- attività propedeutiche all'avvio dell'anno scolastico,
- attività educativa, didattica, di valutazione,
- attività di orientamento e certificazione delle competenze,
- gestione del contenzioso (reclami, esposti, ricorsi, provvedimenti disciplinari, ect.)
- attivazione di organismi collegiali;
- attività didattica relativa a situazione di handicap.

3. Modalità di trattamento dei dati:

	In forma cartacea	*In forma elettronica*
1. Raccolta	- presso gli interessati - presso terzi - tramite schede - per via telefonica - presso registri, elenchi, atti o documenti pubblici	per via telematica
2. Registrazione	- su supporto cartaceo	su supporto elettronico (server, CD rom, dischetti)
3. Organizzazione	- aggregazione di dati - elaborazione in forma cartacea - trasformazione in forma anonima - creazione di profili	aggregazioni di dati elaborazione in forma elettronica trasformazione in forma anonima creazione di profili
4. Conservazione / modifica	- in archivi cartacei (v. titolario) chiusi a chiave	in archivi elettronici (ND, CD, FD) protetti da password
5. Consultazione / estrazione / utilizzo	- accesso autorizzato al titolario	accesso con credenziale all'archivio elettronico
6. Cancellazione / distruzione	utilizzo degli appositi distruggi documenti	eliminazione dei dischetti usati per archiviare dati sensibili e giudiziari

4. **Natura dei dati:**
   - Nominativo indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita; indirizzo privato, indirizzo di lavoro, numero di telefono o di fax o posta elettronica; posizioni rispetto agli obblighi militari; numero di carta di identità, passaporto,patente di guida; numero di posizione previdenziale o assistenziale).
   - Codice fiscale ed altri numeri di identificazione personale (carte sanitarie).
   - Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli soggetti a carico, consanguinei, altri appartenenti al gruppo famigliare).
   - Lavoro (occupazione attuale, precedente; formazione professionale; curriculum lavorativo, competenze professionali).
   - Istruzione e cultura (curriculum di studi e accademico; titolo di studio).

Sono da considerare dati sensibili: origini razziali ed etniche, convinzioni religiose ed adesione ad organizzazione a carattere religioso, stato di salute, convinzioni politiche, dati giudiziari e quindi da conservare in archivi separati e chiusi a chiave se cartacei o protetti da particolare credenziale di autenticazione se elettronici.

5. **Comunicazione e diffusione**:
   - agli Enti Locali per la fornitura dei servizi ai sensi del D.Lgs. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
   - ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
   - alle USL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la preparazione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n. 104;
   - alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente la carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio;
   - agli istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;
   - all'INAIL per la denuncia di infortuni ex D.P.R. 30 giugno 1965, n. 1124;
   - ad aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro, ai sensi della Legge 24 giugno 1997, n. 196 e del D. Lgs. 21 aprile 2005, n. 77 e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizio;
   - alle Avvocature dello Stato, per la difesa erariale e consulenza presso gli organi di giustizia;
   - alle Magistrature ordinarie ed amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione giudiziaria;
   - ai liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza;
   - particolari forme di trattamento e operazioni eseguite.

6. Luoghi ove risiedono i dati
Archivio cartaceo: archivio storico; ufficio della Didattica nell'archivio corrente (schedari, armadi, computers); ufficio del DSGA (armadi e armadio blindato).
Archivio informatico.

Banca Dati: PERSONALE

1. Fonte normativa
T.U. 16.4.1994 n.297, T.U. artt. 309 e 310, D.P.R.22.12.1967 n.1518, D.P.R. 26.1.1999 n.355, Legge 5.2.1992 n.104, D.P.R. 31.8.1999 n.394, D.P.R. 24.7.1977 n.616, L.5.6.1930 n.824, D.P.R. 12.2.1985 n.104, D.P.R. 21.7.1987 n.339

2. **Finalità trattamento:**
   - Trattamento giuridico ed economico del personale e dei collaboratori esterni
   - Gestione previdenziale e pensionistica
   - Reclutamento, selezione, valutazione e monitoraggio del personale
   - Aggiornamento e formazione professionale
   - Adempimento di obblighi fiscali e contabili
   - Adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali
   - Gestione del contenzioso e dei procedimenti disciplinari
   - Attivazione di organismi collegiali.
   - gestione dati inerenti lo stato di salute per esigenze amministrative del personale, assunzioni del personale appartenente alle c.d. categorie protette, igiene e sicurezza sul luogo di lavoro, equo indennizzo, cause di servizio ecc.,

3. Modalità di trattamento dei dati:

	In forma cartacea	***In forma elettronica***
1. Raccolta	- presso gli interessati - presso terzi - tramite schede - per via telefonica - presso registri, elenchi, atti o documenti pubblici	- per via telematica
2. Registrazione	- su supporto cartaceo	- su supporto elettronico (server, CD rom, dischetti, …)
3.Organizzazione	- aggregazione di dati - elaborazione in forma cartacea - trasformazione in forma anonima - creazione di profili	- aggregazioni di dati - elaborazione in forma elettronica - trasformazione in forma anonima - creazione di profili
4. Conservazione / modifica	- in archivi cartacei (cartelle del personale) chiusi a chiave	- in archivi elettronici (ND, CD, FD) protetti da password

5. Consultazione / estrazione / utilizzo	- accesso autorizzato alle cartelle	- accesso con credenziale all'archivio elettronico
6. Cancellazione / distruzione	- utilizzo degli appositi distruggi documenti	- eliminazione dei dischetti usati per archiviare dati sensibili e giudiziari

4. **Natura dei dati:**
   - Nominativo indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita; indirizzo privato, indirizzo di lavoro, numero di telefono o di fax o posta elettronica; posizioni rispetto agli obblighi militari; numero di carta di identità, passaporto,patente di guida; numero di posizione previdenziale o assistenziale).
   - Codice fiscale ed altri numeri di identificazione personale (carte sanitarie).
   - Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli soggetti a carico, consanguinei, altri appartenenti al gruppo famigliare).
   - Lavoro (occupazione attuale, precedente; informazione sulla formazione professionale; curriculum lavorativo, competenze professionali).
   - Istruzione e cultura (curriculum di studi e accademico; titolo di studio).

Sono da considerare dati sensibili: origini razziali ed etniche; convinzioni religiose ed adesione ad organizzazione a carattere religioso; stato di salute; convinzioni politiche; dati giudiziari e quindi da conservare in archivi separati e chiusi a chiave se cartacei o protetti da particolare credenziale di autenticazione se elettronici.

5. Comunicazione e diffusione:
   - agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgsl. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
   - ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
   - alle USL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la preparazione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n. 104;
   - alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente la carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio;
   - agli istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;
   - all'INAIL per la denuncia di infortuni ex D.P.R. 30 giugno 1965, n. 1124;
   - ad aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro, ai sensi della Legge 24 giugno 1997, n. 196 e del D. Lgsl. 21 aprile 2005, n. 77 e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizio;
   - alle Avvocature dello Stato, per la difesa erariale e consulenza presso gli organi di giustizia;
   - alle Magistrature ordinarie ed amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione giudiziaria;
   - ai liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza;
   - particolari forme di trattamento e operazioni eseguite.

6. Luoghi ove risiedono i dati
Archivio cartaceo: archivio storico; ufficio del Personale nell'archivio corrente (schedari, armadi, computers); ufficio del DSGA (armadi e armadio blindato).

Archivio informatico

Banca Dati: CONTABILITA'

1. Fonte normativa
T.U. 16.4.1994 n.297, T.U. artt. 309 e 310, D.P.R.22.12.1967 n.1518, D.P.R. 26.1.1999 n.355, Legge 5.2.1992 n.104, D.P.R. 31.8.1999 n.394, D.P.R. 24.7.1977 n.616, L.5.6.1930 n.824, D.P.R. 12.2.1985 n.104, D.P.R. 21.7.1987 n.339

2. **Finalità trattamento:**
   - Trattamento giuridico ed economico del personale e dei collaboratori esterni
   - gestione stipendiale e previdenziale
   - aggiornamento e formazione professionale
   - adempimento di obblighi fiscali e contabili
   - adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali
   - gestione contratti esperti esterni
   - gestione per le negoziazioni e relative modalità di pagamento rispetto a forniture di beni, servizi o di opere, ovvero proposte ed offerte inerenti le medesime negoziazioni
   - gestione di incassi e pagamenti.

Istituto di Istruzione Secondaria Superiore
LICEO SCIENTIFICO E CLASSICO STATALE
LEONARDO DA VINCI

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it
Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

3. Modalità di trattamento dei dati:

	In forma cartacea	*In forma elettronica*
Raccolta	- presso gli interessati - presso terzi - tramite schede - per via telefonica - presso registri, elenchi, atti o documenti pubblici	- per via telematica
Registrazione	- su supporto cartaceo	- su supporto elettronico (server, CD rom, dischetti, …)
Organizzazione	- aggregazione di dati - elaborazione in forma cartacea - trasformazione in forma anonima - creazione di profili	- aggregazioni di dati - elaborazione in forma elettronica - trasformazione in forma anonima - creazione di profili
Conservazione / modifica	- in archivi cartacei (v. cartelline del personale) chiusi a chiave	- in archivi elettronici (ND, CD, FD) protetti da password
Consultazione / estrazione / utilizzo	- accesso autorizzato alle cartelline del personale	- accesso con credenziale all'archivio elettronico
Cancellazione / distruzione	- utilizzo degli appositi distruggi documenti	- eliminazione dei dischetti usati per archiviare dati sensibili e giudiziari

4. **Natura dei dati:**
   - Nominativo indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita; indirizzo privato, indirizzo di lavoro, numero di telefono o di fax o posta elettronica; posizioni rispetto agli obblighi militari; numero di carta di identità, passaporto,patente di guida; numero di posizione previdenziale o assistenziale).
   - Codice fiscale ed altri numeri di identificazione personale (carte sanitarie).
   - Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli soggetti a carico, consanguinei, altri appartenenti al gruppo famigliare).
   - Lavoro (occupazione attuale, precedente; informazione sulla formazione professionale; curriculum lavorativo, competenze professionali).
   - Istruzione e cultura (curriculum di studi e accademico; titolo di studio).

   Sono da considerare dati sensibili: origini razziali ed etniche; convinzioni religiose ed adesione ad organizzazione a carattere religioso; stato di salute; convinzioni politiche; dati giudiziari e quindi da conservare in archivi separati e chiusi a chiave se cartacei o protetti da particolare credenziale di autenticazione se elettronici.

5. Comunicazione e diffusione:
   - agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgs. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
   - ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
   - alle USL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la preparazione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n. 104;
   - alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente la carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio;
   - agli istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;
   - all'INAIL per la denuncia di infortuni ex D.P.R. 30 giugno 1965, n. 1124;
   - ad aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro, ai sensi della Legge 24 giugno 1997, n. 196 e del D. Lgsl. 21 aprile 2005, n. 77 e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizio;
   - alle Avvocature dello Stato, per la difesa erariale e consulenza presso gli organi di giustizia;
   - alle Magistrature ordinarie ed amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione giudiziaria;
   - ai liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza;
   - particolari forme di trattamento e operazioni eseguite.

6. Luoghi ove risiedono i dati

Archivio cartaceo: Archivio storico; Ufficio della contabilità nell'archivio corrente (schedari, armadi, computers); Ufficio del DSGA (armadi e armadio blindato).

Archivio informatico

Istituto di Istruzione Secondaria Superiore
LICEO SCIENTIFICO E CLASSICO STATALE
LEONARDO DA VINCI

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it
Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

Banca Dati: FORNITORI DI BENI E SERVIZI

1. **Fonte normativa**
   T.U. 16.4.1994 n.297, T.U. artt. 309 e 310, D.P.R.22.12.1967 n.1518, D.P.R. 26.1.1999 n.355, Legge 5.2.1992 n.104, D.P.R. 31.8.1999 n.394, D.P.R. 24.7.1977 n.616, L.5.6.1930 n.824, D.P.R. 12.2.1985 n.104, D.P.R. 21.7.1987 n.339

2. **Finalità trattamento:**
   - Adempimenti di obblighi fiscali e contabili
   - Gestione documenti di trasporto, fatture e note accredito;
   - Gestione richieste preventivi e offerte a fornitori attivi e/o potenziali
   - Gestione fornitori.

3. **Modalità di trattamento dei dati:**

	In forma cartacea	*In forma elettronica*
1. Raccolta	- presso gli interessati - presso terzi - tramite schede - per via telefonica - presso registri, elenchi, atti o documenti pubblici	- per via telematica
2. Registrazione	- su supporto cartaceo	- su supporto elettronico (server, CD rom, dischetti, …)
3. Organizzazione	- aggregazione di dati - elaborazione in forma cartacea - trasformazione in forma anonima - creazione di profili	- aggregazioni di dati - elaborazione in forma elettronica - trasformazione in forma anonima - creazione di profili
4. Conservazione / modifica	- in archivi cartacei (registri) chiusi a chiave	- in archivi elettronici (ND, CD, FD) protetti da password
5. Consultazione / estrazione / utilizzo	- accesso autorizzato ai registri	- accesso con credenziale all'archivio elettronico
6. Cancellazione / distruzione	- utilizzo degli appositi distruggi documenti	- eliminazione dei dischetti usati per archiviare dati sensibili e giudiziari

4. **Natura dei dati:**
   - Nominativo indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita; indirizzo privato, indirizzo di lavoro, numero di telefono o di fax o posta elettronica; posizioni rispetto agli obblighi militari; numero di carta di identità, passaporto,patente di guida; numero di posizione previdenziale o assistenziale).
   - Codice fiscale ed altri numeri di identificazione personale (carte sanitarie).
   - Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli soggetti a carico, consanguinei, altri appartenenti al gruppo famigliare).
   - Lavoro (occupazione attuale, precedente; informazione sulla formazione professionale; curriculum lavorativo, competenze professionali).
   - Istruzione e cultura (curriculum di studi e accademico; titolo di studio).

   Sono da considerare dati sensibili: origini razziali ed etniche, convinzioni religiose ed adesione ad organizzazione a carattere religioso, stato di salute, convinzioni politiche, dati giudiziari e quindi da conservare in archivi separati e chiusi a chiave se cartacei o protetti da particolare credenziale di autenticazione se elettronici.

5. **Comunicazione e diffusione:**
   - agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgs. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
   - ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
   - alle USL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la preparazione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n. 104;
   - alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente la carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio;
   - agli istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;
   - all'INAIL per la denuncia di infortuni ex D.P.R. 30 giugno 1965, n. 1124;

- ad aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro, ai sensi della Legge 24 giugno 1997, n. 196 e del D. Lgsl. 21 aprile 2005, n. 77 e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizio;
- alle Avvocature dello Stato, per la difesa erariale e consulenza presso gli organi di giustizia;
- alle Magistrature ordinarie ed amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione giudiziaria;
- ai liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza;
- particolari forme di trattamento e operazioni eseguite.

6. Luoghi ove risiedono i dati

Archivio cartaceo: Archivio storico; Ufficio della Contabilità nell'archivio corrente (schedari, armadi, computers); Ufficio del DSGA (armadi e armadio blindato).

Archivio informatico

PERSONALE DOCENTE

I dati personali e/o sensibili trattati dai docenti sono:

- i dati personali comuni utilizzati per l'attività didattica e/o organizzativa
- i dati particolari quali quelli deducibili da:
- informazioni contenute nelle comunicazioni scuola –famiglia;
- motivazione assenze per motivi familiari e/o personali;
- note disciplinari trascritte nei trascritte nei registri di classe o nei provvedimenti di sospensione, ecc. (dato particolare in quanto la sua diffusione potrebbe ledere la dignità dell'interessato e il suo diritto alla riservatezza);
- valutazioni intermedie e finali, nonché votazioni, sul profitto, il grado di impiego, la condotta, di ogni alunno assegnato (dati particolari la cui diffusione potrebbe ledere la dignità dell'interessato e il suo diritto alla riservatezza);
- elaborati scritti, in particolare temi di italiano riportati in taluni casi informazioni delicate sulla sfera personale e familiare (dati particolari di grado elevato).

Sono dati sensibili quelli relativi a:

- scelta dell'alunno di avvalersi dell'insegnamento della Religione Cattolica (dati sensibili in quanto idonei a rilevare con buona probabilità le convinzioni religiose);
- giustificazioni di assenze dovute a festività religiose non cattoliche (festività ebraiche, ecc.): dato sensibile in grado di rilevare la convinzione religiosa;
- giustificazione di assenze dovute a motivi di salute (in quanto in taluni casi idoneo a rilevare parzialmente lo stato di salute) visione di certificati medici di avvenuta guarigione (dato particolare o sensibile in quanto parzialmente idoneo a rilevare lo stato di salute);
- certificazioni mediche per esonero da educazione fisica con diagnosi (dato sensibile in quanto idoneo a rivelare lo stato di salute);
- documentazione per l'integrazione di alunni disabili (dato sensibile in quanto idoneo a rilevare lo stato si salute).

Costituiscono occasioni di trattamento dei dati da parte dei docenti quelle in cui essi sono chiamati a:

1. gestire:

- registri di classe, contenenti dati comuni e particolari (certificati medici contenuti in una busta nell'ultima pagina del registro);
- registro del docente in cui sono annotati dati comuni e particolari;
- registro dei verbali dei Consigli di Classe (dati di tipo comune e particolari), normalmente conservato a cura del Responsabile del trattamento in armadio chiuso a chiave, quando esso è affidato al verbalizzatore e/o al coordinatore di classe;
- registri e i documenti in occasione di esami e concorsi;
- elenchi di alunni, dipendenti e genitori per attività varie della scuola;
- dati comuni degli alunni in caso di visite d'istruzione o viaggi.

2. trattare dati personali in occasione della partecipazione a:

- commissioni scolastiche;
- all'organizzazione delle elezioni degli organi collegiali (dati comuni);
- ad attività di gestione del sindacato interno, con conoscenza di dati anche sensibili;
- alla realizzazione delle attività previste dal POF;
- rapporti di continuità nel passaggio degli studenti da un Istituto all'altro.

Per quanto riguarda le modalità di raccolta dei dati si precisa che essi provengono:

- dall'ufficio di segreteria o dalla visione di dati presenti nel Fascicolo Personale detenuto dalla scuola;
- da comunicazioni scritte dalla famiglia o da comunicazioni verbali dello studente;
- dai certificati medici (in casi di esonero da Educazione Fisica) forniti dell'ufficio di segreteria;
- da certificati medici di giustificazione delle assenze esibiti dallo studente stesso;
- da elaborati, forniti direttamente dall'interessato.

I documenti che contengono i dati trattati dai docenti sono conservati in aula docenti, in contenitori chiusi con chiave custodita dal singolo docente autorizzato allo specifico trattamento.

Istituto di Istruzione Secondaria Superiore
LICEO SCIENTIFICO E CLASSICO STATALE
LEONARDO DA VINCI

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it
Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

COLLABORATORI SCOLASTICI

I dati personali e/o sensibili trattati dai collaboratori scolastici sono quelli contenuti nei documenti che essi sono incaricati di ricevere, trasportare, consegnare, inviare aperti o collocati in busta chiusa, in particolare:

a. elenchi di alunni, dipendenti e genitori per attività varie della scuola;
b. certificati medici contenuti nella busta allegata al registro di classe che al termine delle lezioni vengono consegnati ai collaboratori scolastici; questi li pongono nell'armadio destinato alla loro custodia, mentre il registro viene riposto, in custodia, negli scaffali del bancone del centralino;
c. dati personali che sono visionati allo scopo di dare indicazioni di massima agli utenti.

Costituiscono occasione di trattamento dei dati da parte dei collaboratori scolastici quelle in cui essi sono chiamati a svolgere attività di supporto a tutti i trattamenti svolti nella scuola e in particolare:

a. custodire documenti e registri per brevi periodi
b. fotocopiare e faxare documenti contenenti dati personali
c. collaborare ad operazioni di archiviazione di documenti cartacei e/o imputazione di dati negli archivi elettronici.
d. collaborare ad operazioni di scarto ed eliminazione di documenti cartacei
e. collaborare alla gestione di tutti gli archivi cartacei dislocati lontano dalla segreteria.

I documenti che contengono i dati trattati dai collaboratori scolastici sono conservati negli armadi e cassetti delle scrivanie ubicati nei corridoi dei rispettivi reparti che sono chiusi a chiave.

Istituto di Istruzione Secondaria Superiore
LICEO SCIENTIFICO E CLASSICO STATALE
LEONARDO DA VINCI

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it
Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

Allegato B

Istruzioni operative per la sicurezza dei dati

Questo documento fornisce agli incaricati del trattamento informazioni sulle loro responsabilità rispetto alla gestione ed alla sicurezza dei dati trattati dall'Istituto in particolare riguardo:

Integrità: le informazioni devono essere esatte ed aggiornate e non alterabili da incidenti o abusi;

Riservatezza: prevenzione contro l'accesso non autorizzato alle informazioni, quindi i trattamenti devono essere leciti e conformi alle finalità della raccolta;

Disponibilità: il sistema deve essere protetto da interruzioni impreviste e perdite di informazioni.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; nel momento in cui le informazioni raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.
Per garantire sicurezza cioè integrità, esattezza e aggiornamento dei dati, nonché trattamenti leciti e conformi alle finalità della raccolta il personale docente ed ATA uniforma il proprio comportamento professionale alle indicazioni sotto impartite.

Profilo: PERSONALE DOCENTE

Incaricato del trattamento dei dati sotto elencati è individuato l'intero corpo insegnante. Pertanto ogni docente, nel momento in cui è assegnato a far parte del corpo insegnante diventa automaticamente Incaricato di tali trattamenti e riceve dal Responsabile del trattamento le istruzioni scritte sotto impartite:

1. Al fine di garantire il diritto alla protezione dei dati e all'identità personale, nel trattamento dei dati i docenti sono tenuti a:
   - procedere alla raccolta dei dati con la massima cura verificando l'esattezza dei dati stessi;
   - procedere all'aggiornamento dei dati, ove necessario, qualora vengano svolte operazioni dinamiche di trattamento.
2. Al fine di garantire il diritto alla riservatezza i docenti si adoperano per:

   a. Prevenire la diffusione illecita di dati personali e sensibili, avendo cura di accedere ai soli dati, la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità di cui al provvedimento di incarico.

   b. Custodire i dati trattati con mezzi non elettronici avendo cura di:
      - conservare i documenti o atti che contengono dati personali o sensibili o giudiziari in contenitori chiusi a chiave;
      - distruggere o comunque rendere illeggibili, prima di essere eliminati o cestinati i documenti cartacei, non più utilizzati;
      - non lasciare dischetti, fogli, cartelle e quant'altro a disposizione di estranei;
      - non lasciare incustoditi i registri didattici nonché inibirne la consultazione a terzi non autorizzati;
      - conservare i registri didattici nell'apposito armadietto avendo cura di chiuderlo a chiave. Data la natura pubblica di tale documento esso deve essere sempre aggiornato, e a disposizione del Dirigente Scolastico che può in ogni momento prenderne visione e quindi deve essere conservata, con la dovuta cautela, la chiave di riserva dell'armadietto stesso dal Responsabile del trattamento.
      - raccogliere nel registro di classe, in un'apposita busta chiusa apposta nell'ultima pagina di tale registro, i certificati medici che vengono utilizzati per giustificare le assenze. Durante l'orario delle lezioni questi registri sono in classe sulla scrivania, affidati all'insegnante di turno. Al termine delle lezioni un collaboratore scolastico, incaricato del trattamento, raccoglie i certificati medici contenuti nella busta e li ripone nell'armadio con chiave destinato alla loro custodia, mentre il registro viene riposto, in custodia, negli scaffali del bancone del centralino;
      - consultare e poi restituire alla segreteria i certificati medici per esonero da educazione fisica o limitazione dell'attività e in genere i certificati medici e altri documenti, di natura sensibile e non, relativi a particolari interventi didattici e all'integrazione di alunni portatori di handicap.
      - custodire in archivio sicuro gli elaborati degli studenti nei casi contenessero dati particolari. Nel caso si tratti di dati sensibili, consegnarli in busta chiusa alla segreteria per una conservazione a parte.

   c. Custodire i dati trattati elettronicamente avendo cura di seguire il *Disciplinare interno* per l'utilizzo delle strumentazioni informatiche, della rete Internet e della posta elettronica.

   d. Prevenire la comunicazione illecita di dati personali avendo cura di:
      - mantenere il riserbo su informazioni ricevute oralmente;
      - non fornire dati e informazioni di carattere sensibile per telefono, qualora non si abbia la certezza assoluta sull'identità del destinatario;
      - evitare di inviare per fax documenti in chiaro contenenti dati sensibili, nel caso sostituire il nome del soggetto interessato con codice identificativo e quindi inviare la copia della documentazione contrassegnata dal codice, senza il nominativo dell'interessato;

- qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia, richiedere l'identità del chiamante, quindi richiamare avendo così la certezza sull'identità del richiedente.

3. Al fine di monitorare e valutare l'efficacia del piano di protezione dei dati personali è necessario comunicare per iscritto al Responsabile del Trattamento eventuali difformità dei dati trattati o nel funzionamento degli elaboratori.

Istruzioni specifiche sul trattamento dei dati sensibili e giudiziari

Relativamente ai dati sensibili e giudiziari forniti dagli alunni e dalle famiglie e nell'espletamento delle attività connesse alla funzione docente, la S.V. effettuerà i trattamenti consentiti indicati nelle schede, allegate al Regolamento, n. 4 (attività propedeutiche all'inizio dell'anno scolastico),n. 5 (attività educativa, didattica e formativa, di valutazione) e n.7 (rapporti scuola famiglie: gestione del contenzioso) per le finalità di rilevante interesse pubblico indicate e limitatamente ai tipi di dati trattati ed alle operazioni che sono precisate sia come particolari forme di trattamento che come altre tipologie più ricorrenti di trattamento.

Profilo: ASSISTENTE AMMINISTRATIVO

Incaricato del trattamento dei dati sottoelencati è l'unità organizzativa denominata "assistenti amministrativi". Pertanto ogni unità di personale, nel momento in cui è assegnata a tale ruolo diventa automaticamente incaricata del trattamento, manuale o mediante strumenti informatici, e riceve dal Responsabile del trattamento le istruzioni scritte sotto impartite:

1. Al fine di garantire il diritto alla protezione dei dati e all'identità personale
   - procedere alla raccolta dei dati con la massima cura verificando l'esattezza dei dati stessi;
   - procedere all'aggiornamento dei dati su richiesta degli interessati o comunque quando a conoscenza della variazione.

2. Al fine di garantire il diritto alla riservatezza
   - prevenire la diffusione illecita di dati personali sensibili avendo cura di accedere ai soli dati personali, oggetto di trattamento e la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità di cui al provvedimento di incarico.
   - custodire i dati trattati su formato cartaceo avendo cura di:
     a. prelevare dagli archivi i soli atti e documenti necessari,
     b. conservare i documenti nelle attrezzature d'ufficio dotate di serratura e regolarmente chiuse, durante l'intero svolgimento delle operazioni di trattamento;
     c. conservare i documenti o atti che contengono dati sensibili o giudiziari separatamente, in archivi separati (ad esempio stanze, armadi, schedari, contenitori in genere) chiusi a chiave e nei quali devono essere riposti al termine della giornata di lavoro e sempre prima di assentarsi dal posto di lavoro, anche se temporaneamente ed anche qualora l'incaricato debba continuare ad utilizzarli in periodi successivi;
     d. distruggere o comunque rendere illeggibili, prima di essere eliminati o cestinati i documenti cartacei, non più utilizzati;
     e. non lasciare dischetti, fogli, cartelle e quanto altro a disposizione di estranei;
     f. restituire prontamente all'archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative al termine del trattamento;
   - custodire i dati trattati elettronicamente avendo cura di seguire il Disciplinare interno per l'utilizzo delle strumentazioni informatiche, della rete Internet e della posta elettronica.
   - prevenire la comunicazione illecita di dati personali avendo cura di:
     a) non fornire dati e informazioni di carattere sensibile per telefono, qualora non si abbia la certezza assoluta sull'identità del destinatario;
     b) evitare di inviare per fax documenti in chiaro contenenti dati sensibili, nel caso sostituire il nome del soggetto interessato con codice identificativo e quindi di inviare la copia della documentazione contrassegnata dal codice, senza il nominativo dell'interessato;
     c) qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia, richiedere l'identità del chiamante, quindi richiamare avendo così la certezza sull'identità del richiedente.

3. Al fine di monitorare e valutare l'efficacia del piano di protezione dei dati personali:
   a) comunicare per iscritto al Responsabile del Trattamento eventuali difformità dei dati trattati o nel funzionamento degli elaboratori;
   b) aggiornare il registro di carico e scarico per la registrazione delle richieste di comunicazione della documentazione, contenente dati sensibili.

Istruzioni specifiche sul trattamento dei dati sensibili e giudiziari

Relativamente ai dati sensibili e giudiziari di tutti i soggetti con i quali l'istituzione scolastica entra in relazione per i suoi fini istituzionali, la S.V. effettuerà, qualora assegnato a settori di lavoro che li richiedano, i trattamenti consentiti indicati nelle schede, allegate al Regolamento, n.1 (Selezione e reclutamento a tempo indeterminato e determinato e gestione del rapporto di lavoro), n.3 (Organismi collegiali e commissioni istituzionali) n. 4 (attività propedeutiche all'inizio dell'anno scolastico) e n. 5 (attività educativa, didattica e formativa, di valutazione), per le finalità di rilevante interesse pubblico indicate e limitatamente ai tipi di dati trattati ed alle operazioni che sono precisate sia come particolari forme di trattamento che come altre tipologie più ricorrenti di trattamento.

Istituto di Istruzione Secondaria Superiore
LICEO SCIENTIFICO E CLASSICO STATALE
LEONARDO DA VINCI

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it
Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

Profilo: COLLABORATORI SCOLASTICI

Incaricato del trattamento dei dati sotto elencati è l'unità organizzativa denominata "collaboratori scolastici". Pertanto ogni unità di personale, nel momento in cui è assegnata a tale ruolo diventa automaticamente incaricata del trattamento e riceve dal Responsabile del trattamento le istruzioni scritte sotto impartite:

1. A fine di garantire il diritto alla protezione dei dati e all'identità personale, i collaboratori scolastici nel trattamento dei dati sono tenuti a:
   - procedere alla raccolta dei dati con la massima cura verificando l'esattezza dei dati stessi;
   - procedere all'aggiornamento dei dati, ove necessario, qualora vengano svolte operazioni dinamiche di trattamento.
2. Al fine di garantire il diritto alla riservatezza i collaboratori scolastici si preoccupano di:
   - prevenire la diffusione illecita di dati personali sensibili avendo cura di:
     a. accedere ai soli dati personali, oggetto di trattamento, la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità di cui al provvedimento di incarico;
     b. impedire l'ingresso nei locali che sono stati loro affidati in custodia di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, ricordando che:
        - al di fuori dell'attività lavorativa i locali adibiti ad ufficio devono essere chiusi a chiave;
        - durante l'orario di apertura degli uffici il normale livello di vigilanza è svolto dal personale in servizio …….;
        - l'accesso agli uffici è consentito solo al personale dipendente nei tempi e nei modi stabiliti dal DS.
        - gli utenti esterni (alunni, genitori, ecc.) non possono accedere all'area degli uffici se non accompagnati da personale dipendente;
        - i locali adibiti ad archivio devono essere chiusi a chiave anche durante l'attività lavorativa e il solo personale amministrativo è autorizzato ad accedere agli archivi;
        - tenere chiuso a chiave il locale dei server e consentire l'accesso solo alle persone incaricate dal responsabile del trattamento o dall'amministratore di sistema;
     c. impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia di dati nei locali che sono stati affidati loro in custodia da parte di persone non autorizzate secondo quanto stabilito dal Responsabile del Trattamento;
   - custodire i dati trattati con mezzi non elettronici avendo cura di:
     a. conservare i documenti o atti che contengono dati sensibili o giudiziari negli archivi (stanze, armadi, schedari, contenitori in genere) individuati e chiusi a chiave secondo le istruzioni impartite dal Responsabile del trattamento;
     b. distruggere o comunque rendere illeggibili, prima di essere eliminati o cestinati i documenti cartacei, non più utilizzati;
     c. non lasciare dischetti, fogli, cartelle e quant'altro a disposizione di estranei;
     d. non lasciare incustoditi i registri didattici ricevuti in temporanea consegna nonché inibirne la consultazione a terzi non autorizzati;
   - prevenire la comunicazione illecita di dati personali facendo attenzione a:
     a. non fornire dati e informazioni di carattere personale o sensibile per telefono, qualora non si abbia la certezza assoluta sull'identità del destinatario e la legittimità della richiesta;
     b. evitare di inviare per fax documenti in chiaro contenenti dati sensibili, nel caso sostituire il nome del soggetto interessato con codice identificativo e quindi inviare la copia della documentazione contrassegnata dal codice, senza il nominativo dell'interessato;
     c. qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia, richiedere l'identità del chiamante, quindi richiamare avendo così la certezza sull'identità del richiedente;
4. Al fine di monitorare e valutare l'efficacia del piano di protezione dei dati personali comunicare per iscritto al Responsabile del Trattamento eventuali difformità dei dati trattati o nel funzionamento degli elaboratori.

Istituto di Istruzione Secondaria Superiore
LICEO SCIENTIFICO E CLASSICO STATALE
LEONARDO DA VINCI

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it
Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

Allegato C

Lista degli incaricati del trattamento e dei manutentori del sistema
Estremi dei provvedimenti adottati (*All.B D.Lgs. 196/03)*

Data Provvedimento	Tipo Provvedimento	Oggetto	Soggetti autorizzati	Banca dati del trattamento
Prot. N. 2853 Del 16/05/2016	Decreto del Titolare	Nomina del RESPONSABILE al trattamento di dati personali E CUSTODE delle password	Direttore SGA Rag. Vito Antonio ATTOLLINO	Contabilità ed Emolumenti
Prot. N. 2489 Del 16/05/2016	Decreto del Titolare	Incarico di Amministratore di Sistema	Prof. Leonardo CAMPANALE	Personale in servizio, Fornitori (beni e servizi), alunni, contabilità ed emolumenti
Prot. N. 2854 Del 16/05/2016	Decreto del Titolare	Nomina di Incaricato al trattamento dei dati del sistema di videosorveglianza	Prof. Elio RACANO	Personale in servizio, alunni
Prot. N. 2850 Del 16/05/2016	Nota del Responsabile al Trattamento	Individuazione degli incaricati al trattamento di dati personali da parte (assistenti amministrativi)	n. 6 Personale tecnico e amministrativo	banca dati personale direttivo, insegnante e ATA; banca dati fornitori (beni e servizi), banca dati protocollo; banca dati alunni;
Prot. N. 2852 Del 16/05/2016	Nota del Responsabile al Trattamento	Individuazione degli incaricati al trattamento di dati personali da parte (docenti)	n.68 Docenti in servizio	Banca dati alunni e loro familiari;
Prot. N. 2851 Del 16/05/2016	Nota del Responsabile al Trattamento	Individuazione degli incaricati al trattamento di dati personali da parte (Collaboratori Scolastici)	n. 7 Collaboratori Scolastici in servizio	Alunni e Personale

Il Titolare del trattamento
Dott.ssa Daniela CAPONIO
(Dirigente Scolastico)

Istituto di Istruzione Secondaria Superiore
LICEO SCIENTIFICO E CLASSICO STATALE
LEONARDO DA VINCI

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it
Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

Disciplinare interno per l'utilizzo delle strumentazioni informatiche, della rete internet e della posta elettronica da parte del personale e degli studenti

Premesso che compete al datore di lavoro:

- assicurare la funzionalità delle strumentazioni informatiche in dotazione all'Istituto ;
- adottare idonee misure di sicurezza per garantire la disponibilità e l'integrità dei sistemi informativi e dei dati, nonché per prevenire utilizzi indebiti;
- adottare limiti e cautele per evitare la registrazione e diffusione di fotografie e i filmati in tempo reale anche utilizzando i terminali di nuova generazione applicati alla telefonia mobile;
- indicare in modo particolareggiato quali siano gli strumenti messi a disposizione le modalità di utilizzo nell'organizzazione dell'attività lavorativa e/o di studio degli strumenti messi a disposizione dei dipendenti e degli studenti ritenute corrette;
- precisare in che misura e con quali modalità vengano effettuati i controlli;
- tutelare i lavoratori interessati nel trattamento di dati per finalità di gestione del rapporto in ambito pubblico, adottando quelle misure che garantiscono un elevato standard di sicurezza e garanzia;
- tener conto della normativa in tema di informazione, concertazione e consultazione delle organizzazioni sindacali,

sono stabilite le prescrizioni del presente disciplinare di seguito riportate che si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati del trattamento dati in attuazione del D.Lgs. 30 giugno 2003 n. 196 e del Disciplinare tecnico (Allegato B al citato decreto legislativo) e a cui devono attenersi tutti gli utilizzatori (personale e studenti, d'ora in poi definiti *utenti*) delle strumentazioni informatiche, della rete internet e della posta elettronica.

Finalità

Il presente regolamento disciplina le modalità di accesso e di uso della Rete Informatica, telematica e dei servizi che, tramite la Rete stessa, è possibile ricevere o offrire all'interno e all'esterno dell'Istituto per dare il supporto informativo, documentario, alla ricerca, alla didattica, all'aggiornamento e alle attività collaborative tra scuole ed enti, nonché per tutti gli adempimenti amministrativi di legge.

Via Padre Angelo Centrullo 70020 Cassano delle Murge (Ba)
tel. 080 763 790 / 080 776 060
www.liceocassano.it • bais03100g@istruzione.it
Distretto 14 • Cod. Mecc. BAIS03100G • Cod. Fisc. 91 00 14 50 724

Ambito di applicazione

La Rete dell'IISS "Leonardo da Vinci" di Cassano delle Murge è costituita dall'insieme delle risorse informatiche, cioè

- dalle componenti hardware/software e dagli apparati elettronici collegati alla Rete Informatica dell'Istituto
- dall'insieme delle banche dati in formato digitale ed in generale di tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

Il presente regolamento si applica, senza distinzione di ruolo e/o livello, a tutti gli *utenti* interni (personale amministrativo, docenti e collaboratori scolastici) autorizzati ad accedere alla Rete della scuola nell'ambito della propria attività lavorativa ordinaria e straordinaria e agli studenti nei limiti loro assegnati a scopi didattici ed educativi.

Analogamente il presente regolamento si applica alle ditte che effettuano attività di manutenzione, agli eventuali altri soggetti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle convenzioni stesse nel rispetto del presente disciplinare tecnico e a tutti i collaboratori dell'Istituto a prescindere dal rapporto contrattuale con gli stessi intrattenuto (es. soggetto in stage, ecc.).

Principi generali

L'IISS "Leonardo da Vinci" prevede l'utilizzo delle strumentazioni informatiche, della rete Internet e della posta elettronica da parte degli *utenti* quali strumenti utili a perseguire le proprie finalità istituzionali e prevede che lo stesso si conformi ai seguenti principi:

1. ***principio di necessità***: i sistemi informativi e I programmi informatici vengono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
2. ***principio di correttezza***: le caratteristiche essenziali dei trattamenti sono rese note ai lavoratori;
3. ***principio di pertinenza e non eccedenza***: i trattamenti sono effettuati per finalità determinante, esplicite e legittime e i dati sono trattati nella misura meno invasiva possibile.