

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

INDICE

- ▶ Elenco dei trattamenti di dati personali (regola 19.1.)
- ▶ Distribuzione dei compiti e delle responsabilità (regola 19.2.)
- ▶ Analisi dei rischi che incombono sui dati (regola 19.3.)
- ▶ Misure in essere e da adottare (regola 19.4.)
- ▶ Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5.)
- ▶ Pianificazione degli interventi formativi previsti (regola 19.6.)
- ▶ Trattamenti affidati all'esterno (regola 19.7.)
- ▶ Cifratura dei dati o separazione dei dati identificativi (regola 19.8.)

Allegati al presente documento, di cui costituiscono parte integrante:

- All. 1 : Descrizione analitica dei trattamenti di dati personali eseguiti in forma cartacea o elettronica
- All. 2 : Descrizione dei locali in cui vengono trattati dati personali e analisi dei rischi fisici
- All. 3 : Descrizione dei computer con cui vengono trattati dati (e descrizione se appartengono a reti interne chiuse e se sono collegati con l'esterno tramite Internet o la rete intranet del Ministero Pubblica Istruzione)
- All. 4 : Descrizione degli archivi cartacei ed elettronici esistenti e utilizzati, indicazione degli Incaricati di ciascun trattamento, analisi dei rischi fisici dei locali che li ospitano, individuazione degli archivi ad accesso controllato.
- All. 5 : Descrizione delle procedure di sicurezza utilizzate
- All. 6 : Descrizioni delle comunicazioni di dati anche ai fini della verifica di legittimità e dell'adozione di apposito regolamento
- All. 7 : Mansionario delle funzioni in relazione al trattamento dei dati e piano di formazione differenziato in relazione alle funzioni stesse
- All. 8 : Piano operativo per il back-up,
- All. 9 : Misure incrementative della sicurezza dei dati
- All.10 : Verifica sistema di autorizzazione

OGGETTO E FINALITÀ

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

Scuola Statale Direzione Didattica 2° Circolo, con sede in Chieri - Codice fiscale **82001630019**, il cui Rappresentante Legale pro-tempore è il Dirigente Scolastico **VIORA Liliana**, Codice fiscale **VRILLN 52E70D933K**

Il Titolare ha nominato un Responsabile per la sicurezza, nella persona della sig.ra **VASCHETTI Piera**, Codice fiscale **VSCPRI56B48C627M**, Direttore Generale dei Servizi Amministrativi, Dipendente a tempo indeterminato di questa Amministrazione, nominato con lettera prot. N. 2570 a 36 del 30.06.2004 che ha collaborato alla stesura del presente documento e lo firma in calce insieme al Titolare.

Descrizione della sede fisica e della struttura organizzativa. La scuola è così articolata:

sede	N° classi	N° alunni	Dirigente Scolastico	Docenti	educa tori	Personale ATA	volontaria
Via N.S.SCALA 77	19	397	1	49	2	20	1

Vengono indicati inoltre i plessi che ospitano scuole dipendenti dall'Istituto, ove i dati contenuti ed i rischi per l'integrità dei dati medesimi sono ridottissimi:

nei plessi vengono custoditi i registri di classe che contengono i dati anagrafici ed i recapiti delle famiglie degli alunni. Sono presenti n° 1/2 computers utilizzati per la didattica, ma nessuno di essi contiene dati personali

Plesso Porta Garibaldi	N° sezioni	N° alunni	Docenti	educatori	Personale ATA	volontaria
Strada vicinale della Serra	7	166	15	2	6	1
Plesso ANDEZENO primaria	N° classi	N° alunni	Docenti	educatori	Personale ATA	
Via Cesole 2	19	397	11	2	3	
Plesso ANDEZENO infanzia	N° sezioni	N° alunni	Docenti		Personale ATA	
Via Cesole 10	2	52	5		1	
Plesso ARIGNANO primaria	N° classi	N° alunni	Docenti		Personale ATA	
Via Lisa 18	5	51	7		1	
Plesso ARIGNANO infanzia	N° sezioni	N° alunni	Docenti		Personale ATA	
Via Roma 5	2	41	3		1	
Plesso MARENTINO primaria	N° classi	N° alunni	Docenti		Personale ATA	
Piazza Umberto 2	5	62	7		2	
Plesso MARENTINO infanzia	N° sezioni	N° alunni	Docenti		Personale ATA	
Via Roma 24	2	38	5		2	
Plesso MORIONDO primaria	N° classi	N° alunni	Docenti		Personale ATA	
Via MATTA 3	2	51	7		1	
Plesso MORIONDO infanzia	N° sezioni	N° alunni	Docenti		Personale ATA	
Via MATTA 5	2	27	3		1	
Plesso MONTALDO primaria	N° classi	N° alunni	Docenti		Personale ATA	
Via TRINITA' 17	2	17	4		1	
Plesso PAVAROLO primaria	N° classi	N° alunni	Docenti		Personale ATA	
Via MAESTRA 37	5	61	6		1	
plesso PAVAROLO infanzia	N° sezioni	N° alunni	Docenti		Personale ATA	
Via BARBACANE 2	2	48	5		1	

Regola 19.1 - Elenco dei trattamenti di dati personali

Elenco dei trattamenti: informazioni di base.

I provvedimenti organizzativi disposti e le misure di sicure di sicurezza adottate in osservanza a quanto disposto dal D. L.vo 196/2003 sono finalizzati a garantire a ciascun "interessato" (utente, dipendente, fornitore) la tutela di:

- ⊗ Rispetto della privacy, della riservatezza dei dati, della tutela della dignità personale, dell'identità personale;
- ⊗ Rispetto della riservatezza, con riguardo alla tutela dei dati personali, anche allo scopo di evitare l'ingerenza di terzi;
- ⊗ Tutela della riservatezza delle documentazioni custodite dalla scuola e salvaguardia dell'integrità nel tempo delle documentazioni medesime, siano esse costituite da materiale cartaceo che registrate su supporti informatici.

Tabella 1.1: informazioni di base.

<p>T r . 1</p> <p>Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente</p>		<p>Dirigente Scolastico DSGA e Segreteria Amministrativa</p>	<p>C D o o l c l u a m b e o n r t a i t c o a r r i t d a e c l e D i . S r . e . g . R i S s P t P r e i a e</p>
	<p>S-G-N-X</p>		<p>d c d o e m t p t u i t S e P r P s . . M I e n d t i r c a o n C e o t m p e t e n t e</p>

T r . 2	DIPENDENTI E ASSIMILATI: <i>Gestione del</i> contenzioso e procedimenti disciplinari	S-G	Dirigente Scolastico DSGA e Segreteria Amministrativa	UD f o f c i u c m i e o n s t c i o c l a r s t a i c e o i P e r c o o v m i p n u c t i e a r l s
				e - a r e a c o n t e n z i o s o

<p>Organismi collegiali e commissioni istituzionali</p>		<p>Dirigente Scolastico DSGA e Segreteria Amministrativa</p>	<p>C o l l a b o r a t o r i d e l D S S D o c e n t i</p>
	<p>N</p>		<p>i C o l l a b o r a t o r i s c o l a s t i c i m</p>

<p>T r . 4</p>	<p>Attività propedeutiche all'avvio dell'anno scolastico</p>	<p>S-G-N-X</p>	<p>Dirigente Scolastico DSGA e Segreteria Amministrativa</p>	<p>C D o o l c l u a m b e o n r t a i t c o a r r i t d a e c l e D i . S r . e . g . D i o s c t e r n i t e</p>
				<p>i c . o C m o p l u l t a e b r o s r a t o r i s c o l a s t i c i .</p>

<p>T Attività educativa, didattica e formativa, di r valutazione · 5</p>		<p>Dirigente Scolastico DSGA e Segreteria Amministrativa</p>	<p>C o l l a b o r a t o r i d e l D · S · · D o c c e n t i</p>
	<p>S-G-N-X</p>		<p>i · C o l l a b o r a t o r i s c o l a s t i c i · m</p>

T r . 7	Rapporti scuola - famiglie: gestione del contenzioso	S-G-N-X	Dirigente Scolastico DSGA e Segreteria Amministrativa, Docenti	D o c u m e n t i c a r t a c e i e c o m p u t e r s
------------------	--	---------	--	---

Identificativo del Trattamento Descrizione sintetica	Natur a dei dati tratta ti	Struttura di riferimento	Altre strutture concorrenti al trattamento	Descrizione degli strumenti utilizzati
T r . 8 F i t o r i e c c l i e n t i	S-G-N	Dirigente Scolastico DSGA e Segreteria Amministrativa	Collaboratori del D.S., Docenti nelle commissioni, Membri di organi Collegiali, Collaboratori scolastici,	Documenti cartacei e computers

T G r e . s 9 t i o n e f i n a n z i a r i a e c o n t a b i l e	N	Dirigente Scolastico DSGA e Segreteria Amministrativa	Collaboratori del D.S. Membri di organi Collegiali	Documenti cartacei, registri e computers
T G r e . s 1 t 0 i o n e I s t i t u z i o n a l e	S-G-N-X	Dirigente Scolastico DSGA e Segreteria Amministrativa	Collaboratori del D.S.	Documenti cartacei, e computers

T G r e s t i o n e s i t o w e b d e l l ' i s t i t u t o	N	Dirigente Scolastico Incaricati sito web		e computers	

Tabella 1.2. Elenco dei trattamenti con strumenti elettronici: descrizione degli strumenti utilizzati

Identificativo del Trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
-----------------------------------	-------------------------	---	---	----------------------------------

Tr.1	- Archivio SQLDatabase software "Argo" /Pc server - Archivio SIMPI/ rete intranet.	Ufficio blindato	Computer internet	Intranet - rete locale
Tr.2	files di testo	Uffici di segreteria	Computer	rete locale
Tr.3	files di testo	Uffici di segreteria	Computer	rete locale
Tr.4	- Archivio SQLDatabase software "Argo" /Pc server - file di testo/Pc Marg.	Ufficio blindato	Computer	rete locale
Tr.5	File di testo/Pc Marg.	Ufficio blindato	Computer	rete locale
Tr.7	File di testo/Pc Marg.	Ufficio blindato	Computer	rete locale
Tr.8	- Archivio SQLDatabase software "Argo" /Pc server	Ufficio blindato	Computer	rete locale
Tr.9	- Archivio SQLDatabase software "Argo" /Pc server	Ufficio blindato	Computer	rete locale
Tr.10	- Archivio SQLDatabase software "Argo" /Pc server	Ufficio blindato	Computer	rete locale
Tr.11		Laboratorio informatica	Computer	Internet

Tabella 1.3 Elenco della base dati informatiche

LEGENDA:

<p>PCx=codice del computer (v.allegato 3) con i relativi codici descrittivi es. PC03-I-R1-S, segue il segno dei 2 punti per separarlo dal codice dell'archivio. AP= armadio di protezione dati + numero progressivo. Esso non raccoglie necessariamente un archivio omogeneo ma soprattutto dati, materiali, floppy disk e CD che abbisognano di un grado elevato di protezione o di archiviazione separata. Tale armadio deve disporre di serratura robusta, deve stare di regola chiuso, trovarsi preferibilmente in una stanza ben protetta dalle intrusioni, la chiave deve essere gestita dal Titolare, dal Responsabile (se esiste) ed eventualmente da un Incaricato responsabilizzato e che riceva adeguate istruzioni. AE= archivio elettronico informatico + numero progressivo (es. AE03 AB= dischi di backup di archivio elettronico informatico + numero progressivo AD= dispositivo di Backup</p>	<p>Descrizione della tipologia di dato trattato: N= Comune o neutro, S= Sensibile G= Giudiziario X= Sensibile relativo a stato di salute o abitudini sessuali P= Dato degno di particolare protezione. <u>Esempio finale</u> : PCx-R1-I:AE01(NSGXP)</p>	
	<p>Ubicazione fisica</p>	<p>Tipologi a dati trattati</p>
<p>Tr. 4, Tr.5, Tr.7, Anagrafica/carriera Alunni</p>	<p>PCServer-AP264-AESQLDatabas e Argo-AB2-</p>	<p>N-S-G-X</p>
<p>Tr. 1, Stipendi Dipendenti</p>	<p>PCServer-AP264-AESQLDatabas e Argo-AB2-</p>	<p>N-S-X</p>
<p>Tr. 1, Assenze Dipendenti</p>	<p>PCServer-AP264-AESQLDatabas e Argo-AB2-</p>	<p>N-G-X</p>
<p>Tr. 8, Tr.9, Gestione Finanziaria/contabilità</p>	<p>PCServer-AP264-AESQLDatabas e Argo-AB2-</p>	<p>N-G</p>
<p>Tr. 4, Tr. 5, Storico Anagrafica/carriera Alunni</p>	<p>PCServer-AP264-AESQLDatabas e Argo-AB2-</p>	<p>N-S-G-X</p>
<p>Tr. 1, Storico Stipendi Dipendenti</p>	<p>PCServer-AP264-AESQLDatabas e Argo-AB2-</p>	<p>N-S-X</p>
<p>Tr. 1, Storico Assenze Dipendenti</p>	<p>PCServer-AP264-AESQLDatabas e Argo-AB2-</p>	<p>N-G-X</p>
<p>Tr. 8, Tr.9, Storico Gestione Finanziaria/contabilità</p>	<p>PCServer-AP264-AESQLDatabas e Argo-AB2-</p>	<p>N-G</p>
<p>Tr. 1, Tr. 4, Tr. 5, Tr. 7, Tr. 8, Tr. 9, Archivio Corrente Posta Elettronica</p>	<p>PCmargherita-AP264-AB1-ADsoftware Cobian</p>	<p>N-X</p>

Tr. 10, Archivio Corrente/Storico Protocollo informatico	PCServer- AP264- AESQLDatabas e Argo-AB2-	N
Tr. 1, Tr. 4, Tr.5, Tr.7, Tr. 8, Tr.9, Archivio Storico Posta Elettronica	PCmargherita- AP264-AB1- ADsoftware Cobian	N-X
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) memorizzato nel computer	PCmargherita	S-G-X-N
(Trattamenti: Tutti) Storico Documenti elettronici vari (word,excel e simili) memorizzato nel computer	nessuno	
(Trattamenti: Tutti) Storico Documenti elettronici vari (word,excel e simili) memorizzato in floppy disk o CD [o CD] collocati nell'Armadio Protezione Dati	AP264	S-G-X-N
(Trattamenti: Tr.1, Tr2, Tr4, Tr5, Tr.7) Archivio elettronico <u>separato o cifrabile</u> (dati sulla salute o abitudini sessuali) Documenti elettronici vari (word,excel e simili) memorizzati nel computer	PCServer- AP264- AESQLDatabas e Argo	S-G-X-N
(Trattamenti: Tr.4, Tr.5, Tr.7) Backup di Anagrafica/carriera Alunni,armadio di protezione dati	AP264	N
(Trattamenti: Tr.1) Backup di Stipendi Dipendenti:armadio di protezione dati	PCServer- AP264- AESQLDatabas e Argo	N
(Trattamenti: Tr.1) Backup di Presenze Giornaliere Dipendenti:armadio di protezione dati	PCServer- AP264- AESQLDatabas e Argo	N
(Trattamenti: Tr.1) Backup di Assenze Dipendenti:armadio di protezione dati	PCServer- AP264- AESQLDatabas e Argo	S-G-X-N
(Trattamenti: Tr.8, Tr.9) Backup di Gestione Finanziaria/contabilità:armadio di protezione dati	PCServer- AP264- AESQLDatabas e Argo	N

All. 1

ARTICOLAZIONE DEL DOCUMENTO

Conformemente a quanto prescrive il punto 19 del "disciplinare tecnico allegato sub. b) al d.Lgs. 196/2003, nel presente documento sono evidenziati:

1. I dati personali trattati
2. L'indicazione delle sedi e la descrizione dei locali e degli strumenti con i quali si effettuano i trattamenti
3. Il titolare del trattamento dei dati
4. La distribuzione dei compiti e delle responsabilità
5. L'analisi dei rischi che incombono sui dati
6. Le misure adottate e da adottare per garantire l'integrità e la disponibilità dei dati
7. I criteri per l'adozione delle misure minime di sicurezza dei dati;

8. I criteri per la formazione del personale
9. Le dichiarazioni di impegno.

Dati personali in ingresso

I documenti cartacei in arrivo sono sempre consegnati in busta chiusa al dirigente scolastico che li esamina, destinando al protocollo riservato quelli appartenenti alle tipologie di dati riservati o sensibili, e smistando quelli trattati dall'Ufficio di Segreteria.

I documenti ricevuti tramite FAX o consegnati aperti vengono subito recapitati al dirigente scolastico.

Documenti in uscita

I documenti in uscita vengono trattati esclusivamente dal personale incaricato, protocollati e predisposti per la spedizione in busta chiusa. I documenti contenenti dati sensibili vengono chiusi in busta chiusa riservata ed inseriti nel plico contenente la lettera di trasmissione nella quale è evidenziata la presenza di documentazione riservata.

Informazioni sulla tipologia dei documenti e sugli strumenti

Documentazioni complete riguardanti gli alunni, relativi al corso di studi, alla presenza di handicap, alla certificazione dell'idoneità alla pratica sportiva non agonistica, alla scelta dell'insegnamento della religione cattolica. Documenti prodotti dalle famiglie, riguardanti la certificazione della situazione patrimoniale. Tutta la documentazione riguardante i docenti e il personale ATA, con elementi di individuazione di appartenenza sindacale, stato di salute, anche di congiunti per i quali vengono richiesti benefici previsti da particolari norme, allo stato di servizio, alla retribuzione, alle eventuali pratiche disciplinari. Nell'edificio sono presenti n° **30** Computers, di cui **5** negli Uffici di segreteria, tutti collegati in rete che **non** consente l'intraconnessione anche con le postazioni dei laboratori. L'istituto possiede anche un sito web accessibile da internet, ove sono pubblicate notizie riguardanti la didattica, nominativi, elenchi e graduatorie, preventivamente "ripuliti" dei dati personali, foto di alunni, docenti e genitori per le quali sono state acquisite le liberatorie.

Autenticazione informatica

Il controllo degli accessi alle varie postazioni di lavoro viene effettuato mediante l'istituzione di un sistema di autenticazione che permette l'identificazione indiretta del soggetto autorizzato al trattamento dei dati tramite riconoscimento di una credenziale logica costituita da un codice identificativo associato ad una password.

STRUTTURA DEL DOCUMENTO

Nell'impostare la struttura del documento si è tenuto conto degli esempi pubblicati nel sito web del Garante, nonché della "Guida operativa per redigere il documento programmatico".

Vengono, pertanto fornite le seguenti "Informazioni essenziali":

Indicazione della finalità perseguita e dell'attività svolta dall'Istituto:

- Garanzia del servizio scolastico offerto all'utenza dei comuni di appartenenza al Circolo
- Gestione del personale interno con contratto a tempo determinato e indeterminato
- Certificazione degli esiti scolastici e dei servizi prestati dai dipendenti
- Acquisizione di beni e servizi da terzi fornitori

Natura dei dati trattati

dati personali di alunni e dipendenti, tra i quali, assimilabili alla connotazione di "dati sensibili", vengono indicati quelli relativi alla presenza di certificazione della situazione di handicap relativa ad alcuni alunni, alla casuale presentazione di documentazioni prodotte da dipendenti o utenti, recanti notizie sullo stato di salute dei soggetti interessati.

Indicazione della struttura di riferimento

Tutti i dati posseduti dalla scuola vengono trattati esclusivamente presso gli Uffici della sede centrale dell'Istituto, al piano terra dell'edificio di Via **Nostra Signora della Scala 77**, nessuna altra struttura concorre al trattamento dei dati in possesso dell'Istituto.

Descrizione degli strumenti elettronici utilizzati

Computers collegati in rete, forniti di software Explorer per l'accesso ad Internet. Fax per ricezione/ trasmissione di documenti cartacei.

Banca dati

Tutti i dati contenuti in documentazione cartacea vengono raccolti e conservati nell'archivio dell'istituto, classificati e custoditi in appositi schedari. I dati relativi al personale, agli alunni ed alla gestione economico-contabile, anche con riferimento all'identità dei fornitori, sono trattati mediante elaborazione elettronica costituita da software acquisiti dalla ditta Argo-Software.

APPLICABILITÀ

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

Le attività di trattamento prevedono, oltre le tipologie ricorrenti (raccolta, registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione), particolari forme nel caso di dati sensibili e giudiziari, consistenti, secondo quanto indicato nelle schede allegate al Regolamento (D.M. 305/2006), nella comunicazione esclusiva a determinati soggetti e/o categorie di soggetti sottoelencati:

- Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego;
- Organi preposti al riconoscimento della causa di servizio\equo indennizzo, ai sensi del D.P.R. 461\2001;
- Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o infortuni sul lavoro ai sensi del D.P.R. 1124\1965
- Amministrazioni provinciali per il personale assunto obbligatoriamente ai sensi della L. 68\1999;
- Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali;
- Pubbliche Amministrazioni, presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;
- Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai sensi della L. 186\2003;
- Organi di controllo (Corte dei Conti e MEF), al fine del controllo di legittimità e annotazione della spesa dei provvedimenti di stato giuridico ed economico del personale ex L. 20\94 e D.P.R. 38\1998
- Agenzia delle Entrate, ai fini degli obblighi fiscali del personale ex L. 413\1991;
- MEF e INPDAP, per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 335\1995;
- Presidenza del Consiglio dei Ministri per la rivalutazione annuale dei permessi per cariche sindacali e funzioni

pubbliche elettive (art. 50, comma 3, D.Lgs. 165\2001).

- Ministero del Lavoro e delle Politiche Sociali per lo svolgimento dei tentativi obbligatori di conciliazione dinanzi a Collegi di conciliazione ex D.Lgs. 165\2001;
- Organi arbitrali per lo svolgimento delle procedure arbitrali ai sensi del CCNL di settore;
- Avvocature dello Stato, per la difesa erariale e consulenza presso gli organi di giustizia;
- Magistrature ordinarie e amministrative-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione di giustizia;
- Liberi professionisti ai fini del patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale
- Enti Locali per la fornitura dei servizi ai sensi del D.Lgs. 112\1998, limitatamente ai dati indispensabili all'erogazione del servizio;
- Gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali di diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
- ASL e Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la predisposizione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 104\1992;
- 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;
- Istituti di assicurazione per la denuncia di infortuni e per la connessa responsabilità civile;
- Aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro, ai sensi della L. 196\1997 e del D.Lgs. 77\2005 e, facoltativamente, per attività di rilevante di interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizio;
- Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del D.P.R. 445/2000.

4A.3. RIFERIMENTI NORMATIVI

Articolo	Norma
Art. 31	D.Lgs. n. 196/2003
Art. 33- 34-35-36	D.Lgs. n. 196/2003
Allegato B Punti da 19.1. a 19.8	disciplinare tecnico D.Lgs. n. 196/2003
Allegato B Punto 25	D.Lgs. n. 196/2003
Art. 180 (disposizioni transitorie)	D.Lgs. n. 196/2003
Regolamento sul trattamento dei dati sensibili e giudiziari.	D.M. 305/2006

RESPONSABILITÀ

Il titolare è responsabile dell'analisi e della valutazione dei rischi ai fini dell'adozione delle misure di sicurezza,

sia idonee, sia minime. Il titolare si avvale del Gruppo Privacy per la predisposizione della presente modulistica . In particolare il Dirigente scolastico, Titolare del trattamento, deve adottare le misure minime, ai sensi del disciplinare tecnico del D.Lgs. 196/2003, e procedere alla predisposizione delle misure idonee ritenute indispensabili nella struttura. Spetta al titolare del trattamento, coadiuvato dal Gruppo Privacy, valutare la congruità tecnico-economica delle misure proposte e quindi disporre l'adozione delle stesse.

All. 2

Luogo di custodia

Tutti i dati vengono custoditi presso gli Uffici di Via Nostra Signora della Scala n. 77, piano terra.
I locali sono protetti da inferriate metalliche e sistema di antifurto.

Tipologia di accesso

L'accesso agli uffici è consentito solo al personale addetto specificamente incaricato.

Tutti i computer presenti negli Uffici sono bloccati da password di cui sono a conoscenza esclusivamente gli addetti incaricati.

Tipologia di interconnessione

I collegamenti tra le varie postazioni sono resi possibili dalla "rete locale" realizzata mediante cablaggio che consente di raggiungere i vari locali ove sono custodite le postazioni, dalle quali è, peraltro, possibile accedere ad Internet. Non sono presenti dispositivi di collegamento "wireless".

Il Server dell'Ufficio di segreteria e tutti i pc delle varie postazioni, richiedono prima di avviare i programmi la password. L'attivazione della "condivisione" dei dati contenuti nei pc delle varie postazioni di lavoro collegate in rete è limitata solo alle cartelle che non contengono dati personali.

La consegna delle password ai responsabili del trattamento dei dati viene effettuata in forma riservata, con raccomandazione alla custodia.

Viene, altresì disposto il cambiamento delle password ad ogni trimestre.

Settimanalmente i vari responsabili sono incaricati di verificare la possibilità di accesso attraverso la rete ai dati.

INTRODUZIONE ALLA REGOLA 19.2 - 19.3

Identificativo del Trattamento	Natura dei dati trattati	Struttura di riferimento	Altre strutture concorrenti al trattamento	Descrizione degli strumenti utilizzati
Descrizione sintetica	i			

Tr.1	Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc.	S - G - N	Dirigente Scolastico, DSGA e Segreteria, Ufficio Scolastico Regionale della Provincia di Torino - Area personale	Collaboratori del D.S., Collaboratori scolastici, RSPP e addetti SPP	Documenti cartacei, registri e computers
Tr. 2	Dipendenti e Assimilati: Gestione del contenzioso e procedimenti disciplinari	S - G - N	Dirigente Scolastico DSGA e Segreteria	Ufficio Scolastico Regionale della Provincia di Torino - Area contenzioso	Documenti cartacei e computers
Tr. 3	Organismi collegiali e commissioni istituzionali	N	Dirigente Scolastico	Collaboratori del D.S., DSGA e Segreteria, Docenti, Collaboratori scolastici, membri esterni organi collegiali	Documenti cartacei e computers
Tr. 4	Attività propedeutiche all'avvio dell'anno scolastico	N	Dirigente Scolastico DSGA e Segreteria	Collaboratori del D.S., Docenti, Collaboratori scolastici,	Documenti cartacei, registri e computers
Tr. 5	Attività educativa, didattica e formativa, di valutazione	S - N - X - G	Dirigente Scolastico Docenti	Collaboratori del D.S. DSGA e Segreteria , Collaboratori scolastici, membri esterni organi collegiali	Documenti cartacei, registri e computers
Tr. 7	Rapporti scuola - famiglie: gestione del contenzioso	S - G - N - X	Dirigente Scolastico DSGA e Segreteria Docenti,		Documenti cartacei e computers
Tr. 8	Fornitori e clienti	N - G	Dirigente Scolastico DSGA e Segreteria	Collaboratori del D.S., Docenti nelle commissioni, Membri di organi Collegiali, Collaboratori scolastici,	Documenti cartacei e computers
Tr. 9	Gestione finanziaria e contabile	N -	Dirigente Scolastico DSGA e Segreteria	Membri di organi Collegiali	Documenti cartacei, registri e computers
Tr. 10	Gestione Istituzionale	N	Dirigente Scolastico DSGA e Segreteria	Collaboratori del D.S.	Documenti cartacei, registro protocollo informatico
Tr. 11	Gestione sito web dell'istituto	N	Dirigente Scolastico Incaricati sito web		Documenti cartacei e computers

Tipologia di connessione

I computers degli uffici e dei laboratori sono in rete interna, e collegati ad Internet.

MISURE MINIME DI SICUREZZA

Vengono descritte le misure adottate per contrastare i rischi individuati a seguito dell'analisi effettuata e della valutazione degli eventi. Per misura viene inteso lo specifico intervento tecnico informatico ed organizzativo, posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia, nonché per assicurare il livello minimo di protezione.

Vengono indicate, altresì, tutte le attività di verifica e controllo da porre in essere periodicamente, essenziali per assicurare l'efficacia della protezione.

MISURA	RISCHI CONTRASTATI	TRATTAMENTI INTERESSATI	ATTIVAZIONE	STRUTTURA
Istruzioni agli incaricati	Accessi non autorizzati	Tutti	Ottobre 2005	Dirigente scolastico
Incarichi di responsabilità	Deresponsabilizzazione	Tutti	Ottobre 2005	Dirigente scolastico
Formazione	Accessi; Virus;	Tutti	Ottobre 2005	Personale scolastico
Installazione antivirus	Danneggiamento dati informatici	Tutti	Ottobre 2005	Tecnico informatico interno
Potenziamento sicurezza edifici	Incendi ed infiltrazioni	Tutti	Settembre 1979	Dir. Scolastico
Istituzione di Password	Accesso ai dati Informatici	Tutti	Ottobre 2005	Dirigente scolastico, D S G A , Amministrativi
Installazione gruppi di continuità	Danneggiamento banche dati informatici	Tutti	Ottobre 2004	Tecnico informatico interno

Regola 19.2 - Distribuzione dei compiti e delle responsabilità

Tabella 2.1. Strutture preposte ai trattamenti.

STRUTTURA	RESPONSABILE	TRATTAMENTI OPERATI DALLA STRUTTURA	COMPITI DELLA STRUTTURA
Dirigente Scolastico	Titolare del trattamento dei dati	Tutti	Direzione generale di tutte le attività, gestione delle pratiche riservate
Incaricati interni, unità organizzative omogenee:			
1. Collaboratori del DS	Titolare del trattamento dei dati	Tutti (potenzialmente)	Affiancamento al D.S. con deleghe parziali e sostituzione dello stesso in caso di assenza
2. Segreteria	Responsabile del trattamento dei dati	Tutti In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente

3. Corpo Docente	Titolare del trattamento dei dati	Tr.3, Tr.4, Tr.5, Tr.7, Tr.8, In casi eccezionali: Tr.5 (dati sensibili). Se membri di commissione acquisti Tr. 9 (dati giudiziari).	Insegnamento e attività integrative e collaterali, partecipazione alle scelte organizzative e di orientamento generale, partecipazione alla gestione di specifiche attività (Biblioteca, scelte degli acquisti, commissioni varie, ecc.)
4. Collaboratori scolastici o personale ausiliario	Responsabile del trattamento dei dati	Tutti, ma solo con attività di supporto.	Apertura e chiusura della sede, custodia e controllo, consegna e ricezione plichi e lettere, pulizia, assistenza a tutte le altre attività, gestione di dati comuni di alunni, docenti e familiari
5. Membri ESTERNI di Organi Collegiali	Titolare del trattamento dei dati	Tr.3 e tutti gli altri (limitatamente alle strette esigenze della funzione)	Partecipazione alle attività gestionali e alle scelte organizzative e di orientamento generale, nonché il CDI e la GE decisioni di tipo amministrativo, finanziario, regolamentare

STRUTTURA	RESPONSABILE	TRATTAMENTI OPERATI DALLA STRUTTURA	COMPITI DELLA STRUTTURA
	incaricati interni con compiti specifici o ulteriori:		

<p>1. Incaricato del Backup per i dati e delle procedure di ripristino</p>	<p>Titolare del trattamento dei dati</p>	<p>Tutti, ma limitatamente alla funzione</p>	<p>Esegue il backup almeno settimanale degli archivi informatici contenenti dati personali. Coordina l'impostazione del piano di recupero in caso di disastro informatico che comporti l'inagibilità del sistema o la perdita di dati personali. Coordina le prove obbligatorie di efficienza del backup e di ripristino dei dati dalla copia di salvataggio.</p>
<p>i p r i s t i n o</p>			

2.

C
u
s
t
o
d
e
d
e
l
l
e
c
h
i
a
v
i
d
e
g
l
i
a
r
c
h
i
v
i
a
d
a
c
c
e
s
s
o
c
o
n
t
r
o
l
l
a
t
o
.
E
v

<p>3.</p> <p>C u s t o d e d e l l e p a s s w o r d s</p>	<p>Titolare del trattamento dei dati</p>	<p>Tutti i trattamenti informatici, ma limitatamente alla funzione</p>	<p>Da ogni Incaricato munito di accesso al computer mediante password, ad ogni scadenza della password (3mesi) riceve una busta chiusa contenente la password, da tenere a disposizione in caso di necessità di accesso agli archivi elettronici del sostituto.</p>

4.

T
e
c
n
i
c
o
i
n
t
e
r
n
o
d
e
l
l
a
M
a
n
u
t
e
n
z
i
o
n
e
d
e
l
S
o
f
t
w
a
r
e

Titolare del
trattamento dei
dati

Tutti, ma limitatamente alla
funzione

Manutenzione del software e piccoli
interventi sull'hardware

<p>5.</p> <p>R . S . P . P . e A d d e t t i a l S . P . P . . R . L . S .</p>	<p>Titolare del trattamento dei dati</p>	<p>I trattamenti relativi all'applicazione della normativa 626 o ad essa riferiti. Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni.</p>	<p>Applicazione normativa Dlgs 626/1994 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale</p>
--	--	---	--

<p>6.</p> <p>R L S - r a p p r e s e n t a n t e d e i l a v o r a t o r i p e r l a s i c u r e z z a</p>	<p>Titolare del trattamento dei dati</p>	<p>Diritto di consultazione di tutti i documenti informatici strettamente inerenti alla funzione e risultanti come diritto di conoscenza</p>	<p>Contributo all'applicazione normativa Dlgs 626/1994 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale; verifica ecc.</p>

7.

D
o
c
c
e
n
t
i
I
n
c
a
r
i
c
a
t
i
d
e
l
l
a
r
e
d
a
z
i
o
n
e
e
g
e
s
t
i
o
n
e
d
i
P
i
a
n
i
E
d
u
c
a

<p>8.</p> <p>P e r s o n a l e i n c a r i c a t o d e l l a c r e a z i o n e</p>	<p>Titolare del trattamento dei dati</p>	<p>tutti i trattamenti informatizzati, relativi all'attività didattica</p>	<p>Creazione e gestione del sito web dell'Istituto</p>
<p>e g e s t i o n e d e l s i t o w e b</p>			

Responsabili interni di trattamento:			
Direttore Generale e dei Servizi Amministrativi	Titolare del trattamento dei dati	Tutti i trattamenti, limitatamente alla gestione amministrativo-contabile e alla gestione delle attività dei Collaboratori Scolastici.	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente
Responsabili esterni di trattamento::			

<p>1.</p> <p>D o c e n t i , e d u c a t o r i , A n i m a t o r i</p>	<p>Titolare del trattamento dei dati</p>	<p>rigorosamente nei limiti relativi alle funzioni: Tr.4 - Tr.5</p>	<p>Gestione di attività teatrali o ludiche o di animazione in favore degli alunni dell'Istituto e supporto educativo</p>
<p>2.</p> <p>G e s t</p>			
<p>o r i d i t r a s p o r t i</p>	<p>Titolare del trattamento dei dati</p>	<p>tutti i trattamenti informatici e non, limitatamente alla funzione</p>	<p>trasporto visite istruzione</p>

<p>3.</p> <p>A p p a l t i p u l i z i a</p>	<p>Titolare del trattamento dei dati</p>	<p>i trattamenti cartacei,</p>	
<p>4.</p> <p>E n t e a s s i c u r a t i v o</p>	<p>Titolare del trattamento dei dati</p>	<p>i trattamenti cartacei, limitatamente alla funzione</p>	<p>Copertura assicurativa Infortuni e Rc del personale ed alunni</p>

Regola 19.3 - Analisi dei rischi che incombono sui dati.

Tabella 3.1. Analisi dei rischi

Evento		Impatto sulla sicurezza dei dati		Riferimento misure d'azione	
		Descrizione		Gravità stimata	
Comportamenti degli operatori	Furto delle credenziali di autenticazione	Accesso non autorizzato al computer	bassa	Istruzioni agli Incaricati (all.5), formazione, azione del "Custode delle Parole-chiave", controllo dell'accesso ai locali che sono chiusi a chiave quando non presidiati, divieto di accesso ai locali alle persone non autorizzate	
	carenza di consapevolezza, disattenzione o incuria	Le credenziali perdono riservatezza o dati sono inutilmente resi visibili	bassa	Come precedente	
	comportamenti sleali o fraudolenti	Accesso per fini personali ai dati (che però sono poco appetibili), che vengono conosciuti da Incaricati che non ne hanno diritto	bassa	Come precedente, inoltre: eventuale creazione di profili di autorizzazione diversificati e utilizzo cifratura per i rari files contenenti dati sensibili, giudiziari o particolari importanti.	
	errore materiale	Cancellazione o perdita di dati	Bassa (esiste copia cartacea e backup di tutto)	Formazione degli incaricati, profilo di autorizzazione che non consenta la formattazione dei dischi fissi o la cancellazione di files importanti.	

Eventi relativi agli strumenti	azione di virus informatici o di codici malefici	Cancellazione di dati, malfunzionamenti o blocco del sistema, trasmissione casuale di dati a indirizzi di posta elettronica memorizzati, confusione con incapacità di individuare dati utili	bassa	Regolare aggiornamento dell'antivirus e del software (patches) , con istruzioni agli incaricati e monitoraggio di controllo sull'effettiva attuazione, istruzioni a individuare e prevenire le situazioni a rischio (vedi allegato 5),
	tecniche di sabotaggio	Confusione con rischio di non individuazione di messaggi utili o di loro cancellazione per errore	Medio/bassa	Formazione degli Incaricati a riconoscere i messaggi di disturbo e a gestire le regole di assegnazione dei messaggi di posta elettronica alle varie cartelle
	malfunzionamento, indisponibilità o degrado degli strumenti	Malfunzionamenti o blocco del sistema	media	Manutenzione programmata, formazione ad individuare i sintomi di malfunzionamento per un rapido intervento, piano di backup - Disaster Recovery e di continuità operativa
	accessi esterni telematici non autorizzati	Visione indebita di dati o sabotaggio	Bassa (i dati non sono appetibili e il loro valore si basa sull'originale cartaceo)	Installazione di Firewall, con regolare aggiornamento
	intercettazione di informazioni in rete	Visione indebita di dati	minima	Eventuale adozione di cifratura o firma elettronica per proteggere i dati più gravi (allo studio)

Eventi relativi al contesto	accessi non autorizzati a locali/reparti ad accesso ristretto	Sabotaggio delle macchine, con eventuale perdita di dati; accesso abusivo se le credenziali fossero lasciate disponibili	bassa	Solidità degli infissi dei locali, chiusura a chiave quando non presidiati installazione di allarme antifurto, disponibilità di estintori ad anidride carbonica per non danneggiare i computers, istruzioni a tutti gli operatori (v. all. 5)
	asportazione e furto di strumenti contenenti dati	Perdita di dati , rallentamento o blocco dell'attività per carenza di computer	Probabilità media, gravità elevata	Come punto precedente, Inoltre, regolare back-up dei dati, piano di back-up - Disaster Recovery e di continuità operativa
	eventi distruttivi, naturali	Perdita di dati , rallentamento o	Probabilità minima	Come punto precedente,
	o artificiali, dolosi, accidentali o dovuti ad incuria	blocco dell'attività per carenza di computer		sensibilizzazione e formazione degli Incaricati e dei Collaboratori Scolastici. Verifica della congruità dei locali rispetto a rischi di infiltrazioni d'acqua, incendio, inondazioni, terremoti . Uso di protezioni antifulmine e contro sovratensioni elettriche. Verifica della logistica degli apparecchi e del loro corretto posizionamento. Custodia dei dischi di back-up in armadio ignifugo, chiusi.
	guasto ai sistemi complementari (impianto elettrico)	Perdita di dati e blocco del sistema	Media	Gruppo di continuità

Istruzioni agli Incaricati (all.5)	Comportamenti inadeguati o errati degli operatori, incuria, ecc. :	Tutti	Tutte	All. 5	Settembre 2004		Titolare, mensilmente
formazione	Furto delle credenziali di autenticazione; carenza di consapevolezza, disattenzione o incuria;	idem	idem	All. 6	Ottobre 2005	aprile 2007	Titolare, semestrale
azione del "Custode delle Parole-chiave",	Comportamenti inadeguati o fraudolenti con dati sensibili (di virus informatici e tecniche di sabotaggio)	idem			Settembre 2005		Titolare, mensilmente
controllo dell'accesso ai locali che sono chiusi a chiave quando non presidiati, divieto	mal funzionamento, indisponibilità o degrado degli strumenti accessi esterni telematici non autorizzati	idem	idem	All. 2	Settembre 2004		Titolare, mensilmente
di accesso ai locali alle persone non autorizzate	intercettazione di informazioni in rete errore materiale						
Misura	Rischio contrastato	Trattamento o interessato	Eventuale banca dati interessata	Rif. Scheda analitica	Misura già in essere (con data di effettività)	Misura da adottare (con data di effettività prevista)	Periodicità e responsabilità dei controlli
eventuale creazione di profili di autorizzazione diversificati	Visione indebita e perdita di dati riservati	Tutti	Tutte	All. 4	Settembre 2004	Integrazione entro ottobre 2007	Titolare, annuale
Utilizzo di files cifrati per i rari files contenenti dati sensibili, giudiziari o particolari importanti.					Non adottato	Se si presenta la necessità	Titolare, annuale
profilo di autorizzazione che non consenta la formattazione dei dischi fissi o la cancellazione di files importanti.		Tutti	idem	All. 4	Settembre 2004		Titolare, annuale

Regolare aggiornamento dell'antivirus e del software (patches) : istruzioni agli incaricati	Eventi relativi agli strumenti: azione di virus informatici o di codici malefici; o altre tecniche di sabotaggio; malfunzionamento, indisponibilità o degrado degli strumenti; accessi esterni telematici non autorizzati; intercettazione di informazioni in rete	tutti	tutte	All. 5	settembre 2004		Titolare, mensile
istruzioni a individuare e prevenire le situazioni a rischio (vedi allegato 5)		idem	idem	All. 5	Settembre 2004		Titolare, semestrale

Misura	Rischio contrastato	Trattamento o interessato	Eventuale banca dati interessata	Rif. Scheda analitica	Misura già in essere (con data di effettività)	Misura da adottare (con data di effettività prevista)	Periodicità e responsabilità dei controlli
formazione degli Incaricati a riconoscere i messaggi di disturbo e a gestire le regole di assegnazione dei messaggi di posta elettronica alle varie cartelle	Eventi relativi agli strumenti: azione di virus informatici o di codici malefici; o altre tecniche di sabotaggio; malfunzionamento, indisponibilità o degrado degli strumenti; accessi esterni telematici	tutti	tutte	All. 5	Settembre 2004		Titolare, semestrale
Manutenzione programmata		idem	idem				Titolare, semestrale
Formazione ad individuare i sintomi di malfunzionamento per un rapido intervento	non autorizzati; intercettazione di informazioni in rete	idem				Settembre 2007	Titolare, annuale
piano di backup - Disaster Recovery e di continuità operativa	idem	idem			Settembre 2004		Titolare, semestrale
Installazione di Firewall, con regolare aggiornamento	idem	idem			Settembre 2004		Titolare, semestrale
Eventuale adozione di cifratura o firma elettronica per proteggere i dati più gravi	idem	idem					Titolare, semestrale

Misura	Rischio contrastato	Trattamento o interessato	Eventuale banca dati interessata	Rif. Schede analitica	Misura già in essere (con data di effettività)	Misura da adottare (con data di effettività prevista)	Periodicità e responsabilità dei controlli
Verifica ed eventuale miglioramento della solidità degli infissi dei locali	Eventi relativi al contesto: accessi non autorizzati a locali/ reparti ad accesso ristretto; asportazione e furto di strumenti contenenti dati; eventi distruttivi,	Tutti	Tutti	All. 2	Settembre 2004		Titolare, semestrale
Chiusura a chiave dei locali quando non presidiati : istruzioni a tutti gli operatori		idem	idem	All. 5	Settembre 2004		Titolare, mensile
installazione di allarme antifurto,	naturali e artificiali, dolosi, accidentali o dovuti ad incuria;	idem					Titolare, annuale
disponibilità di estintori ad anidride carbonica per non danneggiare i computers	guasto ai sistemi complementari (impianto elettrico);	idem					Titolare, annuale
Regolare back-up dei dati, piano di back-up - Disaster Recovery e continuità operativa	errori umani nella gestione della sicurezza fisica	idem			Settembre 2004		Titolare, mensile
Custodia dei dischi di back-up in armadio ignifugo, chiusi, collocato in locale diverso dai computer.	idem	idem			Settembre 2004		Titolare, semestrale
Sensibilizzazione e formazione degli Assistenti Ammvi e dei Collaboratori Scolastici	idem	idem	All. 5		Settembre 2004		Titolare, mensile

Verifica della congruità dei locali rispetto a rischi di infiltrazioni d'acqua, incendio, inondazioni, terremoti	Eventi relativi al contesto: accessi non autorizzati a locali/ reparti ad accesso ristretto; asportazione e furto	idem	idem		Settembre 2004		Titolare, annuale
Uso di protezioni antifulmine e contro sovratensioni elettriche	di strumenti contenenti dati; eventi distruttivi, naturali o artificiali, dolosi, accidentali o	idem	idem		Settembre 2004		Titolare, annuale
Verifica della logistica degli apparecchi e del corretto posizionamento	dovuti ad ingegneria; posto ai sistemi complementari	idem			Settembre 2004		Titolare, semestrale
Gruppo di continuità	(impianto elettrico); errori umani nella gestione della sicurezza fisica	idem				Settembre 2003	Titolare, annuale
A studio una miglior ventilazione dei computers (revisione regolare delle ventole interne e loro potenziamento).	Idem	idem					Titolare, annuale
Formazione e sensibilizzazione di tutti gli Incaricati, compresi Operatori delle pulizie e Collab.Scolastici per il controllo.	Idem	idem			Ottobre 2004		Titolare, mensile
Nuove misure incrementative della sicurezza:							
Soluzioni incrementative della sicurezza	Rischi fisici	idem	idem				Titolare, mensile
Soluzioni incrementative della sicurezza	Rischi sicurezza dati	idem	idem			Ottobre 2007	Titolare, mensile

Regola 19.5 - Criteri e modalità di ripristino della disponibilità dei dati

Tab. 5.1.- Back-up archivi elettronici

Data base	Dati sensibili o giudiziari contenuti	Criteri individuati per il salvataggio (procedure operative in essere)	Ubicazione e di conservazione delle copie	Struttura operativa incaricata del salvataggio
------------------	--	---	--	---

(Trattamenti: Tr. 4, Tr.5, Tr. 7, Anagrafica/carriera Alunni, memorizzato nel computer	PcServer-AESQLdatab ase Argo - AB2	N-S-G-X	Back-up ogni 15 gg., su dischi alternati in modo da utilizzare supporti diversi da quelli utilizzati la volta precedente	AP264	Incaricato : Cerasuolo Margherita
(Trattamenti: Tr.1) Stipendi Dipendenti:memorizzato nel computer	PcServer-AESQLdatab ase Argo - AB2	N-S-X	idem	AP264	Incaricato : Mori Maria Cristina
(Trattamenti: Tr.1) Assenze Dipendenti:memorizzato nel computer	PcServer-AESQLdatab ase Argo - AB2	N-G-X	idem	AP264	Incaricato : Troppino Silvia
Trattamenti: Tr.1) reclutamento Dipendenti:memorizzato nel computer	PcServer-AESQLdatab ase Argo - AB2	S-G-N-X	idem	AP264	Incaricato : Imbrenda Fernanda
(Trattamenti: Tr.9) Gestione Finanziaria/contabilità:memorizzato nel computer	PcServer-AESQLdatab ase Argo - AB2	N-G	idem	AP264	Incaricato : Vaschetti Piera
(Trattamenti: Tr.8) Gestione fornitori e clienti:memorizzato nel computer	PcServer-AESQLdatab ase Argo - AB2	N-G	idem	AP264	Incaricato : Dellabernardina Elida
(Trattamenti: Tr.10) Gestione archivio corrente/storico protocollo informatico	PcServer-AESQLdatab ase Argo - AB2	N	idem	AP264	Incaricato : Cerasuolo Margherita
(Trattamenti: Tr.1, Tr.4, Tr.5, Tr.7, Tr.8, Tr.9) Archivio Corrente Posta Elettronica	PCmargherita - ADsoftware Cobian	N-X	idem	AP264	Incaricato : Cerasuolo Margherita

Tab. 5.2. PIANIFICAZIONE PROVE DI RIPRISTINO DEI DATI

Data base/archivio	Scheda operativa	Pianificazione delle prove di ripristino
(Trattamenti: Tr. 4, Tr.5, Tr.7,) Anagrafica/carriera Alunni, memorizzato nel computer		luglio 2007 - Gennaio 2008
(Trattamenti: Tr.1) Stipendi Dipendenti:memorizzato nel computer		luglio 2007 - Gennaio 2008
(Trattamenti: Tr.1) Assenze Dipendenti:memorizzato nel computer		luglio 2007 - Gennaio 2008
(Trattamenti: Tr.9) Gestione Finanziaria/contabilità:memorizzato nel computer		luglio 2007 - Gennaio 2008

(Trattamenti: Tr.1) Reclutamento Dipendenti:memorizzato nel computer	luglio 2007 - Gennaio 2008
(Trattamenti: Tr.8) Gestione fornitori e clienti:memorizzato nel computer	luglio 2007 - Gennaio 2008
(Trattamenti: Tr.10) Gestione archivio corrente/storico protocollo informatico	luglio 2007 - Gennaio 2008

INTRODUZIONE ALLA REGOLA 19.6

Pianificazione degli interventi formativi previsti

1 Scopo della formazione.

Il dirigente scolastico ha ritenuto che la previsione degli interventi formativi degli incaricati del trattamento, rientra tra gli aspetti più importanti del presente documento programmatico sulla sicurezza, in quanto si può realmente parlare di effettiva sicurezza del trattamento solo in costanza di un dettagliato piano di formazione degli incaricati.

Da quanto evidenziato ne consegue che la predisposizione e l'applicazione di sofisticati strumenti di sicurezza, informatica e non, non garantiscano la stessa in modo assoluto senza le capacità e/o le adeguate conoscenze del personale ATA chiamato alla loro gestione, nonché anche del corpo insegnante per quel che attiene il trattamento dei dati degli alunni effettuato con i registri di classe. Difatti, una gestione impropria da parte di tali soggetti, la mancanza di chiare direttive esplicative e l'assenza di strumenti di controllo di facile e rapida applicazione, costituiscono le cause principali per la verifica anche inconsapevole di danni agli interessati ed in definitiva la causa prioritaria di trattamenti illegittimi e non conformi alle specifiche finalità dell'istruzione scolastica.

Quanto premesso trova effettivo riscontro nel comma 19.6. del D.Lgs. 196/2003 che impone, infatti, "la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali."

2 Tecniche di formazione degli incaricati del trattamento dei dati personali.

Il Dirigente scolastico ha ritenuto necessario ed indispensabile prevedere un adeguato e dettagliato piano di formazione del personale ATA quale incaricato del trattamento dei dati personali e del corpo docente.

Tale intervento formativo è stato predisposto ed applicato sotto la diretta vigilanza e la coordinazione del Responsabile del Trattamento.

Il piano di formazione è articolato in più lezioni, in ognuna delle quali devono essere affrontati specificamente e dettagliatamente gli aspetti più delicati della legge sulla Privacy e sulle misure di sicurezza e ciò al fine di permetterne vari approfondimenti nonché riflessioni e dibattiti.

Per quel che concerne gli insegnanti deve essere rilevato come gli stessi debbano prestare la massima attenzione a custodire il registro di classe durante le ore di lezione, a non permetterne la sua consultazione a soggetti non autorizzati nonché a conservare tale registro al termine delle lezioni negli appositi siti predisposti dal Titolare.

Tra le varie tecniche didattiche il Titolare ed il Responsabile del Trattamento dei dati personali dell'Istituto scolastico, hanno ritenuto più proficua quella della lezione tenuta direttamente dal Responsabile del trattamento medesimo, in base alla sua specifica conoscenza della materia della Privacy e ciò con il supporto di materiale cartaceo esplicativo della Legge sul trattamento dei dati personali e del Regolamento sul trattamento dei dati sensibili e giudiziari. Copia del materiale esplicativo deve essere consegnato agli incaricati presenti alle lezioni di formazione al fine della migliore e più completa comprensione della materia e degli adempimenti richiesti dalla medesima nonché delle misure minime di sicurezza applicate dall'Istituto

scolastico.

3 Valutazione dell'efficienza del piano di formazione

Il Dirigente Scolastico ed il Responsabile del Trattamento dei dati personali dopo avere dettagliatamente individuato il contenuto del piano di formazione del personale ATA e degli insegnanti hanno ritenuto ulteriormente importante approntare una serie di strumenti di verifica dell'efficienza della formazione per essere certi che la formazione impartita sia stata realmente recepita dagli incaricati del trattamento e che sia stata determinante ad un appropriato e sicuro trattamento dei dati personali.

Si è ritenuto che la formazione possa affermarsi e dirsi veramente tale, solo se in grado di soddisfare le esigenze dell'Istituto scolastico per la salvaguardia delle quali è stata prevista l'utilizzazione di un questionario da sottoporre ai partecipanti a fine corso per effettuare una dettagliata valutazione dell'efficacia del loro apprendimento.

4 Aggiornamento e programmi individuali di formazione.

Dopo avere affrontato nel dettaglio l'importanza di tale adempimento deve, comunque, ricordarsi che la formazione deve essere sempre aggiornata in base al disposto del D.Lgs n. 196/2003 in coincidenza con l'obbligo di aggiornamento del Documento Programmatico sulla Sicurezza. Deve tenersi ben presente una chiara distinzione tra:

- A) AGGIORNAMENTO PERIODICO**
- B) AGGIORNAMENTO SPECIFICO**

Per il quale l'aggiornamento periodico deve essere adempiuto sotto la diretta vigilanza del Responsabile del Trattamento con cadenza almeno annuale e quello specifico, viceversa, tempestivamente effettuato ogni qualvolta l'incaricato sia deputato a trattare nuove banche dati oppure utilizzi nuovi strumenti informatici e/ o nuove e diverse procedure.

Muovendo da questa considerazione ne discende che se l'incaricato viene assegnato a nuove mansioni o se viene trasferito da un settore ad un altro, deve essere effettuato un nuovo e specifico aggiornamento mediante un programma individuale che deve essere impartito dal Responsabile in relazione alla nuova e specifica attività di trattamento svolta.

5 Misure di sicurezza suppletive relative al trattamento di particolari dati sensibili.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari richieste dal disciplinare tecnico del D.Lgs. n. 196/2003 ed in particolare dal punto 19.8. per i dati personali idonei a rivelare lo stato di salute. Vengono, individuati dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Una breve parentesi è necessaria per comprendere nel dettaglio gli adempimenti da effettuarsi ed in particolare un riferimento al punto 20 del disciplinare tecnico secondo quale "I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici", ed il successivo punto 21 che stabilisce, inoltre, che "sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati, al fine di evitare accessi non autorizzati e trattamenti non consentiti", oltre ancora il punto 22 secondo il quale "i supporti rimovibili contenenti dati sensibili o giudiziari, se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili".

Per quanto riportato nel detto disciplinare il punto 23 prescrive che, "sono adottate idonee misure per garantire il ripristino dell'accesso ai dati, in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

Per quanto sopra riportato non v'è dubbio che la protezione crittografica dei dati cui si riferisce lo stesso Testo Unico, in materia di trattamento di dati personali, rappresenti un prezioso strumento di tutela e di sicurezza contro i rischi di accesso ai dati personali.

Deve porsi particolare attenzione al trattamento dei dati sensibili poiché debbono essere archiviati nel

sistema informatico centrale con estrema sicurezza perché l'accesso alla consultazione e/o alla modificazione dei dati sensibili sarà sempre condizionato dal rispetto della procedura di identificazione degli incaricati ed in definitiva dei seguenti criteri in base ai quali:

- 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 lettura o cifratura.

Per quanto detto, e per le menzionate procedure gestionali dei dati sensibili, deve evidenziarsi in definitiva che, i dati sensibili debbono essere nettamente separati e gestiti autonomamente ed indipendentemente da ogni incaricato, unicamente in base al proprio profilo di autorizzazione.

Per quel che attiene i dati personali degli alunni riportati sui registri didattici si prevede che, al termine dell'ultima lezione del giorno, l'insegnante abbia cura di riporre i relativi registri nello specifico sito predisposto dal Titolare.

6 INTERVENTI DI COLLABORATORI ESTERNI, ESPERTI E SPECIALISTI

Nel caso in cui l'Istituzione scolastica si dovesse avvalere, per l'attuazione di interventi previsti dall'offerta formativa o dagli interventi miranti all'integrazione dei soggetti diversamente abili, della collaborazione di terapisti, esperti e specialisti, assistenti igienico-personali, è escluso, nei limiti del possibile, l'accesso dei medesimi a documentazioni contenenti dati sensibili. In merito alla possibilità di trattamento di dati personali particolari da parte dei suddetti soggetti, è previsto che i medesimi dichiarino:

1. di essere consapevoli degli obblighi previsti dal D. L.vo 196/2003
2. di impegnarsi ad ottemperare all'obbligo di tutela dei dati personali
3. di adottare le istruzioni specifiche ricevute per la garanzia di sicurezza dei dati

Regola 19.6 - ORGANIGRAMMA FORMAZIONE

INCARICATI INTERNI, UNITA' ORGANIZZATIVE OMOGENEE:	Formazione prevista tra il 31.03.2007 e il 31.3.2008
Collaboratori del DS	<p>Numero persone da formare: 2 Numero di persone già formate: 0 Dato il livello professionale e l'elevata capacità di auto apprendimento sarà prima di tutto fornita il <Kit formazione privacy>, manuale completo divulgativo sulla privacy. Questo avverrà ad inizio anno scolastico, quando i Collaboratori saranno designati. Si cercherà di avviare a corsi di formazione, al momento non conosciuti. Oppure saranno aggregati a corsi organizzati per il personale di segreteria, quando saranno svolte lezioni interessanti anche per la loro funzione.</p>
Segreteria	<p>Numero persone da formare e aggiornare: 3 Numero di persone già formate: 3</p>
	<p>Essendo entrato da poco in vigore (il 30.1.2007) il <REGOLAMENTO DATI SENSIBILI E GIUDIZIARI>, approvato con decreto n. 305 del 7/12/2006 dal Ministero Pubblica Istruzione, la formazione del personale verterà principalmente su questo tema, utilizzando apposito volume illustrativo e riunioni tematiche introdotte dal DGSA :</p> <ul style="list-style-type: none"> - L'informativa sui dati sensibili dopo l'entrata in vigore del Regolamento - Regolamento e gestione alunni - Regolamento e gestione dipendenti - Regolamento e gestione del contenzioso dipendenti, alunni e famiglie - Regolamento e formazione organi elettivi della scuola
Corpo Docente	<p>Numero persone da formare: 24 Numero di persone già formate: 106 Nel corso delle periodiche riunioni degli Organi Collegiali il Titolare illustrerà l'argomento e se ne potrà discutere. Si inviterà anche un esperto per una breve relazione. Si tratterà in particolare del tema: "Dati sensibili: è vietato chiedere agli alunni dati sensibili che non siano strettamente indispensabili per l'attività formativa." E' prevista la distribuzione all'inizio del prossimo anno scolastico (settembre-ottobre) di un opuscolo divulgativo ma esauriente che illustrerà il Codice in materia di protezione dei dati.</p>
Collaboratori scolastici e personale ausiliario	<p>Numero persone da formare: 5 Numero di persone già formate: 26 Viene fornito il <Compendio di livello base > della normativa privacy Ma soprattutto si farà affidamento su alcune riunioni con illustrazione del tema fatta in modo semplice ed elementare da parte del Titolare o del DGSA..</p>

Neo assunti o supplenti temporanei	Viene consegnato il "Kit Formazione privacy", come dispensa. Si tratta di uno strumento per integrare la formazione di chi ha già avuto la formazione di base, ma anche di chi non ha avuto ancora formazione. Trattasi di un sistema modulare di files leggibili al computer o stampabili e riproducibili, che contengono: un manuale breve e facile per gli incaricati che hanno responsabilità meno impegnative in ambito privacy, un manuale completo e approfondito per i responsabili e per gli Incaricati che hanno maggiori responsabilità, oltre 20 schede tematiche per approfondire ciascuno dei temi importanti della Privacy o per aiutare a svolgere determinate mansioni.. Il sistema si presta all'aggiornamento permanente del personale. Può essere anche la base per fare riunioni del personale stesso in cui si discutono le cose lette.
Membri ESTERNI di Organi Collegiali (Consiglio Di Circolo)	Numero persone da formare: 8 Numero di persone già formate: 0 Viene fornito il <Compendio di livello base > della normativa privacy Nel corso delle periodiche riunioni degli Organi Collegiali il Dirigente illustrerà brevemente l'argomento e se ne potrà discutere. Si inviterà anche un esperto per una breve relazione.
INCARICATI INTERNI CON COMPITI SPECIFICI O ULTERIORI:	Formazione prevista tra il 31.03.2007 e il 31.3.2008
Incaricato del Backup periodico e coordinatore del <Disaster recovery> e delle prove di ripristino	[0] Già formato [7] Da formare Viene fornito il Manuale e software per la gestione del Backup generale e in particolare anche dell'archivio di Outlook Express E' previsto un breve colloquio con il DSGA per verifica e approfondimento.
Custode delle chiavi degli archivi ad accesso controllato. E vice-custode delle chiavi.	[1] Già formato [0] Da formare Viene fornito una Guida per una miglior gestione degli archivi E' previsto un breve colloquio con il DSGA per verifica e approfondimento.
Custode delle passwords	[1] Già formato [0] Da formare Viene fornito una guida per una miglior organizzazione della gestione delle passwords. E' previsto un breve colloquio con il DSGA per verifica e approfondimento.
Tecnico interno della Manutenzione del Software	[1] Già formato [0] Da formare Viene fornito il <Compendio di livello avanzato > della normativa privacy E' previsto un breve colloquio con il DSGA per verifica e approfondimento.
R.S.P.P. e Addetti al S.P.P.	[1] Già formato [0] Da formare Viene fornito il <Compendio di livello avanzato > della normativa privacy E' previsto un breve colloquio con il Dirigente per verifica e approfondimento.
Docenti Incaricati della redazione e gestione di Piani Educativi Individuali di alunni con handicap	Numero persone da formare: 10 Numero di persone già formate: 6 Viene fornito il <Compendio di livello avanzato > della normativa privacy E' previsto un breve colloquio con il Dirigente per verifica e approfondimento.
Personale incaricato della creazione e gestione del sito web	Numero persone da formare: 4 Numero di persone già formate: 8 Viene fornito il <Compendio di livello avanzato > della normativa privacy (uno dei files del <Kit formazione privacy>) E' previsto un breve colloquio con il Dirigente per verifica e approfondimento.

ALTRI INCARICATI:	Formazione prevista al momento del conferimento dell'incarico
<ul style="list-style-type: none"> - organizzazione di educatori o Animatori Esterni - Organizzazione autotrasporto privato viaggi d'istruzione - Organizzazione assicurazione infortuni e Rc - Organizzazione pulizia locali scolastici (appalti pulizia art.8 L.124/99) 	Viene fornito il <Compendio di livello base > della normativa privacy E' previsto un breve colloquio con il Dirigente o del DSGA per verifica e approfondimento.
RESPONSABILI INTERNI DI TRATTAMENTO:	Formazione prevista tra il 31.03.2007 e il 31.3.2008
Direttore Generali Servizi Amministrativi	[1] Già formato [0] Da formare E' previsto un breve colloquio con il Dirigente per verifica e approfondimento.

Dichiarazioni finali e di impegno

Obiettivo di questo Istituto è incrementare la sicurezza dei dati su supporto sia informatico che cartaceo e dei relativi archivi, pertanto si è proceduto ad un'attenta verifica delle condizioni di sicurezza degli archivi, in particolare quelli, separati o meno, contenenti dati sensibili/giudiziari.

A seguito dell'analisi, saranno effettuati interventi incrementativi della sicurezza.

Di questo c'è traccia negli allegati di questo documento.

Chieri, 30 marzo 2007

Firma del Titolare: **Liliana VIORA**

Firma del Responsabile: **Piera VASCHETTI**

