



**MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA  
RICERCA**

UFFICIO SCOLASTICO REGIONALE PER LA LOMBARDIA

**SCUOLA MEDIA STATALE "VIRGILIO"  
Via Trebbia, 1 - 26100 CREMONA**

# **Manuale della privacy**

**(applicazione Decreto legislativo 196/2003)**

**Emissione: AMBRO SCUOLE S.R.L. – Milano**

**Verifica: Commissione Privacy d'Istituto**

**Approvazione: Il Titolare del trattamento dati**

## INDICE DEGLI ARGOMENTI:

Premessa	3
Note introduttive	4
PROCEDURA [PRVINF001] BACKUP ATTIVO DEI DATI REV. 1.00	9
PROCEDURA [PRVINF002] DISASTER RECOVERY REV. 1.00	11
PROCEDURA [PRVINF003] GESTIONE DELLE PASSWORD REV. 1.00	12
PROCEDURA [PRVINF004] CREDENZIALI DI AUTENTICAZIONE REV. 1.00	13
PROCEDURA [PRVINF005] AGGIORNAMENTI DEL SOFTWARE REV. 1.00	15
PROCEDURA [PRVGEN001] CUSTODIA CHIAVI REV. 1.00	16
PROCEDURA [PRVGEN002] ACCESSO AI LOCALI REV. 1.00	17
PROCEDURA [PRVINF003] DIVULGAZIONE E TRASM. DATI REV. 1.00	18
PROCEDURA [PRVINF004] INFORMATIVA EX ART. 13 rev. 1.00	19
PROCEDURA [PRVINF005] D.P.S. rev. 1.00	20
PROCEDURA [PRVGEN006] DIRITTI DELL'INTERESSATO REV. 1.00	21

## Premessa

Il presente documento è stato espressamente concepito per fornire una guida organica a chiunque intenda prendere visione e verificare le attività e l'impegno organizzativo dell'Istituto nell'applicazione del Decreto Legislativo 196/2003.

La prima sezione "Note introduttive" è di riepilogo rispetto alle prerogative di applicazione del Codice, e vuole fornire un breve vademecum di applicazione.

Per la programmazione delle attività si fa riferimento al Documento Programmatico sulla Sicurezza.

Per le attività dei Soggetti preposti al trattamento si fa riferimento alle lettere d'Incarico agli stessi inviate.

Sono incluse nel presente manuale le procedure per:

### Trattamenti informatizzati:

Procedure	Codice di riferimento
Backup dei dati	Prvinf001
Disaster recovery	Prvinf002
Gestione delle password	Prvinf003
Custodia delle credenziali di autenticazione	Prvinf004
Gestione degli aggiornamenti del software	Prvinf005

### Altre procedure e documenti:

Procedure e documenti	Codice di riferimento
Custodia chiavi locali ad accesso riservato	Prvgen001
Accesso ai locali da parte di personale non autorizzato	Prvgen002
Divulgazione e trasmissione dati	Prvgen003
Informativa art. 13 (utenza e dipendenti)	Prvgen004
Documento Programmatico sulla Sicurezza	Prvgen005
Procedura di esercizio dei diritti ex art. 7	Prvgen006

La stesura delle procedure pur tenendo conto delle specificità degli strumenti tecnici e delle scelte organizzative operate, vuole consegnare agli Incaricati una guida applicabile indipendentemente dall'hardware, dal software o dallo specifico strumento adottato. Le specificità e le soluzioni tecniche di dettaglio, sono rimandate ed affrontate nelle corrispondenti sessioni formative e per descrizione nelle sezioni di competenza del Documento programmatico sulla Sicurezza.

## NOTE INTRODUTTIVE

Il trattamento della privacy è regolato dal D.Lgs 30/06/2006 n. 196, il cui articolo 1 recita:

*"Chiunque ha diritto alla protezione dei dati personali che lo riguardano"*

Le norme distinguono i *dati* in:

<i>Dati Personali</i>	qualunque informazione relativa a persona fisica o giuridica, anche indirettamente identificabile mediante riferimento a qualsiasi informazione.
<i>Dati Identificativi</i>	i dati personali che permettono l'identificazione diretta della persona.
<i>Dati Sensibili</i>	relativi ad origine razziale, religione, politica, appartenenza ad organizzazioni a vario titolo, stato di salute, sessualità.
<i>Dati giudiziari</i>	Sentenze, condanne ed anche i semplici certificati del casellario.

Vengono individuate alcune *figure*, che effettuano il trattamento dei dati, e che lo "subiscono":

<i>Titolare del trattamento</i>	persona fisica o giuridica cui competono le decisioni in merito al trattamento dei dati
<i>Responsabile</i>	persona fisica o giuridica preposto dal titolare al trattamento dei dati
<i>Incaricato</i>	persona fisica autorizzata a compiere materialmente le operazioni di trattamento dei dati
<i>Interessato</i>	la persona fisica o giuridica i cui dati vengono trattati

Viene fatta distinzione tra i *principi* di:

<i>Comunicazione</i>	mettere a conoscenza dei dati una determinata persona
<i>Diffusione</i>	mettere a disposizione di soggetti indeterminati i dati

Sono considerate *Misure Minime*:

le misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza della protezione dei dati.

Sono definite:

<i>Autenticazione Informatica</i>	l'insieme degli strumenti elettronici e delle procedure per la verifica dell'identità
<i>Credenziali di Autenticazione</i>	i dati e gli strumenti in possesso di una persona, utilizzabili per l'autenticazione informatica
<i>Parola Chiave</i>	una sequenza di caratteri, componenti una <i>Credenziale di Autenticazione</i> , associata ad una persona
<i>Profilo di Autorizzazione</i>	l'insieme delle informazioni associate ad una persona, che permettono l'identificazione dei dati a questa persona accessibili
<i>Sistema di Autorizzazione</i>	strumenti che abilitano l'accesso ai dati in base al profilo dell'utente

L'*ambito* è stabilito nel territorio dello Stato, anche per dati detenuti all'estero.

Il *trattamento effettuato da persone fisiche per fini personali* è soggetto alla normativa solo in caso di *Comunicazione Sistemática*, o a *Diffusione*.

Sono considerati *Diritti dell'Interessato Art. 7 Codice della Privacy*:

ottenere indicazione di:	Origine dei dati
	Finalità e modalità
	Logica applicata
	Estremi Identificativi del <i>Titolare</i> e dei <i>Responsabili</i>
	Soggetti ai quali possono essere comunicati i dati
	Aggiornamenti, rettifiche ed integrazione dei dati, cancellazione, trasformazione in forma anonima o il blocco dei dati
Opporsi	Per fini legittimi, al trattamento dei dati

*Modalità del Trattamento e Requisiti dei Dati.*

I *Dati Personali* devono essere:

- *Trattati* in modo lecito e secondo correttezza
- Raccolti e *Registrati* per scopi determinati, espliciti e legittimi
- *Esatti ed Aggiornati*
- *Pertinenti, Completi* e non *Eccedenti* rispetto alle finalità per le quali sono stati raccolti
- *Conservati* in forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario agli scopi per i quali sono stati raccolti

L'Interessato o la persona presso la quale sono raccolti i dati deve essere *Previamente Informato* circa:

le *Finalità* e le *Modalità* del trattamento dei dati

- la *Natura Obbligatoria* o *Facoltativa* del conferimento dei dati
- le *Conseguenze* di un eventuale *Rifiuto* di rispondere
- i *Soggetti* o le *Categorie di Soggetti* ai quali i dati possono essere comunicati, e l'*Ambito di Diffusione*
- i suoi *Diritti*
- gli *Estremi Identificativi* del *Titolare* e di un *Responsabile*

In caso di *Cessazione* di un trattamento i dati devono essere:

- Distrutti
- Ceduti ad altro *Titolare*, purché ad un trattamento compatibile con gli scopi per cui sono stati raccolti
- Conservati a scopo puramente personale

Il trattamento dei dati personali è ammesso solo con il *Consenso Espresso* dell'Interessato, *Liberamente* e con *Riferimento* ad un trattamento *Chiaramente Individuato*, *Richiesto* all'Interessato prima della raccolta dei dati, *Documentato* per iscritto, e se sono rese le adeguate *Informazioni* all'Interessato.

Il *Consenso* è *Manifestato* in forma *scritta* quando il trattamento riguarda *Dati Sensibili*.

Il *Consenso* non serve quando il trattamento:

- È necessario per un *Adempimento di Legge*
- È necessario per gli obblighi derivanti da un *Contratto* del quale l'interessato è parte
- Riguarda dati provenienti da *Pubblici Registri*
- Riguarda dati relativi allo svolgimento di *Attività Economiche*
- È necessario per la *Salvaguardia della Vita o dell'Incolumità* di un terzo
- È necessario per perseguire un *Legittimo Interesse*
- È effettuato da *Associazioni o Enti Senza Scopo di Lucro*
- Per *Scopi Scientifici o Statistici*
- È effettuato da *Enti Pubblici*

L'*Organizzazione Interna* riguarda:

- La *Struttura delle Nomine*
- Gli *Aggiornamenti* e le *Revisioni* degli *Adempimenti d'Informativa*, *Gestione del Consenso*
- L' *Informazione e la Formazione del Personale*

*Struttura delle Nomine*

- Obbligatoria: Incaricati del trattamento
- Non Obbligatoria: Responsabile del trattamento

Il *Titolare* del Trattamento deve fornire al *Responsabile* chiara *Identificazione* dei *Compiti* attribuiti, dell'ambito di *Responsabilità*, e porre in essere periodica attività di *Verifica*

Il responsabile deve, a sua volta, identificare i criteri per l'individuazione degli *Incaricati*, in modo da procedere alla nomina di persone preposte al rilevante trattamento di dati personali.

Il Codice distingue tra *Misure di Sicurezza Minime*, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti, di distruzione o perdita dei dati, e di accesso non autorizzato o di trattamento non conforme, e *Misure di Sicurezza Idonee* a ridurre al minimo i rischi.

Il Codice distingue inoltre le *Misure di Sicurezza* in base a Trattamenti con *Strumenti Elettronici*, e Trattamenti con *Strumenti Non Elettronici*

Per i trattamenti con *Strumenti Elettronici*, le *Misure di Sicurezza Minime* sono rappresentate da:

- Autenticazione Informatica
- Gestione delle Credenziali di Autenticazione
- Utilizzo di Sistemi di Autorizzazione
- Aggiornamenti Periodici
- Protezione degli Strumenti Elettronici e dei Dati
- Procedure per la Custodia ed il Ripristino delle Copie di BackUp
- Redazione ed Aggiornamento del Documento Programmatico sulla Sicurezza
- Adozione di tecniche di Cifratura o Codici Identificativi per determinati trattamenti effettuati da Organismi Sanitari

Il *Sistema di Autenticazione Informatica* consente il trattamento dei dati solo agli *Incaricati* in possesso di Codice Identificativo (*UserID*) e Parola Chiave (*Password*), oppure di *Dispositivo di Autenticazione*

Lo *UserID* deve prevedere *Criteri di definizione ed Assegnazione*, e di *Disattivazione*, e deve essere:

- Individuale
- Non riutilizzabile
- A validità limitata nel tempo

La *Password* deve prevedere:

- Criteri di Creazione (almeno 8 caratteri)
- Criteri di Gestione e di Custodia
- Validità temporale
- Modalità di Ripristino in caso di Perdita

Ad ogni *Incaricato* possono essere associate una o più *Credenziali*.

Il Titolare del Trattamento dovrà fornire agli *Incaricati* precise *Istruzioni* in merito a:

- Gestione e Conservazione delle Credenziali
- Custodia dei Dispositivi in possesso ed uso
- Gestione e Custodia degli Strumenti Elettronici
- Individuazione delle Modalità di Accesso

Il Sistema di Autorizzazione prevede:

- Criteri di Individuazione Preventiva
- Verifiche Periodiche
- Criteri di Revoca

Altre *Misure di Sicurezza* previste sono:

- L'aggiornamento e le verifiche periodiche dell'ambito del trattamento consentito agli Incaricati e la redazione della Lista degli Incaricati
- L'installazione e l'aggiornamento di software Antivirus e per la prevenzione della vulnerabilità
- Le istruzioni per il BackUp dei dati
- Le istruzioni per la custodia e l'uso dei supporti rimovibili, per la loro distruzione, e per la cancellazione dei dati ripetuti
- L'adozione di misure idonee al Ripristino dei Dati in caso di danneggiamento

Il trattamento con *Strumenti Non Elettronici* è consentito *solo se* sono adottate le misure minime di sicurezza individuate dal Codice, e con le modalità previste dal disciplinare tecnico All. B.

## PROCEDURA [PRVIN001] BACKUP attivo dei dati rev. 1.00

(regola 19.5, all. B, D. Leg.vo 196/2003)

(Punto 3 Documento Programmatico della Sicurezza, Tabella C301)

Al fine di garantire l'applicazione delle misure minime previste dalla regola 19.5 All. B disciplinare tecnico del D. Leg.vo 196/03, si stabilisce di adottare la seguente procedura:

- Backup incrementale automatizzato file di database dichiarati in tabella C301 del D.P.S. con gestione set di backup
- Copia di archiviazione dei supporti rimovibili in casseforti (possibilmente ignifughe)
- Copia di archiviazione incrementale delocalizzata su server di backup con garanzia di sicurezza fisica e logica.
- Test periodico di ripristino
- Sostituzione periodica dei supporti rimovibili con un nuovo set di backup
- Verifica periodica della disponibilità della copia delocalizzata
- Generazione archiviazione storica semestrale

Sequenza	Azione	Periodicità	Strumento
01	Sostituzione dei supporti rimovibili per il backup.	Giornaliera o a giorni alterni	Cartuccia DAT, CD-rom, DVD-ROM, ecc.
02	Collocamento del supporto rimovibile in casseforti.	Giornaliera o a giorni alterni	Non previsto
03	Verifica della funzionalità del sistema di duplicazione on-line del database.	settimanale	Verifica aggiornamento del file replicato in cartella destinazione.
04	Verifica delle funzionalità di copia del database su supporto rimovibile.	settimanale	Verifica corrispondenza esatta dei files.
05	Verifica della disponibilità della copia delocalizzata.	Settimanale	Archiviazione delle ricevute di buon fine.
06	Verifica della funzionalità del RESTORE del supporto rimovibile: a) porre il database in modalità off-line b) eseguire una copia manuale del DB c) eseguire il restore d) verificare la funzionalità e l'aggiornamento del DB e) ripristinare la copia manuale f) riportare il DB on-line	semestrale	Utility di sistema.
07	Approntare ed etichettare un nuovo set di backup.	Biennale	Non previsto
08	Verificare la disponibilità ed il restore della copia delocalizzata procedendo come da sequenza 06.	Semestrale	Utility di sistema.
09	Archiviare e non utilizzare 1 supporto rimovibile dal set di backup e sostituire	Semestrale	Cartuccia DAT, CD-rom, DVD-

	con un supporto vergine. Etichettare lo stesso come storico semestrale.		ROM, ecc.
10	Archiviare e non utilizzare/cancellare 1 copia delocalizzata riportandola su HD locale o supporto rimovibile. Etichettare lo stesso come storico semestrale.	Semestrale	Utility di sistema.

Per le attività qui illustrate si conferisce incarico specifico ad uno o più Soggetti, per i quali si è previsto adeguato supporto formativo.

La formazione è finalizzata a fornire le linee guida e la consapevolezza necessaria ad adottare il massimo grado di attenzione nell'esecuzione delle procedure stesse, oltre ad illustrare le tecniche che garantiscono il miglior livello di sicurezza.

La formazione viene somministrata dal Responsabile, e viene ripercorsa in ogni caso di nuovo Soggetto/i incaricato e/o d'innovazione tecnologica e procedurale.

I controlli sull'efficacia della procedura e sulla precisa applicazione della stessa, rimangono prerogativa del Titolare del trattamento dati e sono affidati al Responsabile (a nomina indicata sul D.P.S.) così come previsto dal D.P.S.

## PROCEDURA [PRVINFO02] DISASTER RECOVERY rev. 1.00

(regola 19.5, all. B, D. Leg.vo 196/2003)

(Punto 3 Documento Programmatico della Sicurezza, Tabella C301)

La previsione di Legge non solo richiede la puntuale esecuzione delle procedure di backup finalizzate alla conservazione dei dati, ma richiede anche la disponibilità degli stessi nel tempo e comunque per tutta la durata del servizio in erogazione. A tal riguardo è necessario poter dimostrare di aver agito e previsto, al meglio delle possibilità della struttura, le attività di ripristino della disponibilità del servizio a causa di evento distruttivo imprevedibile.

Tale procedura è definita di *Disaster Recovery* ed è in tal senso di tipica derivazione informatica peraltro prassi consolidata per i grandi data-center. In molte situazioni risulta invece una novità introdotta dal Codice della privacy ed in ragione di questo, si stabilisce di fornire al personale preposto adeguato supporto formativo.

Considerata la gravità e l'eccezionalità degli eventi che possono generare l'adozione della procedura qui illustrata, si stabilisce di conferire incarico per l'esecuzione della procedura al Responsabile (a nomina indicata sul D.P.S.), che consultato il Titolare del trattamento dati, dispone tempestivamente:

a) il blocco delle attività di trattamento
b) analisi dei danni subiti e relazione al Titolare
c) denuncia alle Autorità competenti ove previsto
d) denuncia alla compagnie assicurative ove esista copertura
e) comunicazione ad Enti e/o Soggetti/Aziende coinvolti in ragione della proprietà immobiliare/mobiliare dei beni interessati dal disastro
f) Stima dei tempi di ripristino delle infrastrutture danneggiate
g) diffusione informativa sulla sospensione del servizio
h) Stima dei tempi di ripristino degli strumenti preposti al trattamento
i) Analizzare e predisporre se possibile, strumenti alternativi per il periodo di inattività forzata
j) Comunicazione dei tempi di ripristino del servizio parziale o totale
k) Organizzare e supervisionare le procedure di acquisto e ripristino degli strumenti
l) Testare la compatibilità e l'affidabilità dei sistemi ripristinati
m) Convocare l'Incaricato della procedura di restore dei dati ed eseguire la stessa
n) Verificare la disponibilità di tutti i dati e dei corrispondenti servizi
o) Disporre il ripristino delle attività di trattamento
p) Comunicare il ripristino del servizio

Per situazioni di disastro che interessano le infrastrutture tecnologiche, si dispone di organizzare una configurazione minima di replica del sistema che prevede:

- Server delocalizzato con replica dell'active directory di dominio
- Client delocalizzato, configurato per l'accesso ai databases e le utenze di base

Per le situazione di disastro che interessano i trattamenti non informatizzati, si dichiara la definitiva distruzione dei supporti in uso e si dispone l'utilizzo delle copie disponibili.

## PROCEDURA [PRVIN003] gestione delle PASSWORD rev. 1.00

Di seguito vengono illustrate le regole di gestione della password legata ad un profilo di autenticazione personale.

Ogni incaricato può ricevere una o più credenziali di accesso al sistema, ciascuna riferita a diversi profili di autenticazione, generati dal Responsabile in accordo con il Titolare per svolgere i compiti propri delle designazioni d'incarico al trattamento mediate strumenti informatici.

La Password legata alla UserId, consente la riconoscibilità personale. Tutte le attività svolte in sessione d'uso, attivata con una determinata combinazione di UserId e Password, sono direttamente riconducibili alla credenziale di accesso attribuita al singolo Incaricato, che rispetto al suo operato, si assume ogni responsabilità.

Alcune regole fondamentali per la gestione delle password:

- 1) La password deve essere generata dallo stesso incaricato;
- 2) usare una parola chiave di almeno nove caratteri;
- 3) usare una combinazione di caratteri alfabetici e numerici: meglio ancora è inserire almeno un segno di interpunzione o un carattere speciale (per es. [IncSegrDid0@257Af#](#));
- 4) non usare mai il proprio nome o cognome, né quello di congiunti (coniuge, figli, genitori) o di animali domestici.
- 5) È altresì importante curare la conservazione e la segretezza della parola chiave evitando di trascriverla sul classico post-it oppure di tenerla nel portafogli o trascritta nella prima pagina dell'agenda o della rubrica di ufficio.
- 6) La password scade automaticamente ogni 6 mesi, il sistema si occupa di fornire un pro-memoria di scadenza.
- 7) Incaricati con le stesse mansioni ed attività utilizzano UserId e password diverse e personali.
- 8) L'accesso con UserId e Password viene garantito anche da PDL diverse da quelle di utilizzo personale.
- 9) E' obbligatorio sospendere manualmente la sessione d'uso di sistema operativo, quando ci si allontana dalla PDL, premendo contemporaneamente i tasti: [CTRL]+[ALT]+[DEL/CANC]. Premerli nuovamente per riattivare la sessione e poi digitare la password.
- 10) Gestire eventuali codici di cifratura.

## PROCEDURA [PRVINFO04] CREDENZIALI DI AUTENTICAZIONE rev. 1.00

(allegato B del D.Lgs 196/03, regole del punto 10)

Visto il D.Lgs196/2003 art. 31, 33-36 sulle misure minime di sicurezza; Visti gli articoli da 28 a 30 sulle figure responsabili dei trattamenti di dati; Visto il Disciplinare tecnico – allegato B del predetto D.Lgs, in particolare la regola 10:

“10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.”

Si deve pertanto provvedere a nominare il “Custode delle parole-chiave (password)” ed il suo sostituto in caso di assenza.

La funzione di “Custode delle parole-chiave (password)” prevede i seguenti compiti:

- 1) Ricevere da ciascun Incaricato utilizzatore di computer una busta, già chiusa e controfirmata, contenente una sola credenziale (coppia di parola-chiave o password e username o nomeutente o user-id). Se l'utente dispone di diverse credenziali, dovrà ricevere altrettante buste chiuse.
- 2) Ogni busta, naturalmente, dovrà riportare gli estremi identificativi dell'utente della credenziale e il riferimento alla funzione che la credenziale in essa contenuta svolge, ovvero il sistema di accesso alla quale essa fa riferimento.
- 3) La busta chiusa sarà controfirmata anche dal “Custode” e quindi custodita in luogo sicuro di cui il “Custode” sia l'unico detentore della chiave.
- 4) Come previsto dal punto 10 dell'Allegato B, in caso di assenza prolungata dell'incaricato (o suo impedimento) che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il “Custode” aprirà la busta e ne consegnerà il contenuto al Titolare o al Responsabile o all'Incaricato da loro delegato, facendosi rilasciare ricevuta. Avvertirà tempestivamente dell'intervento il detentore originario della parole-chiave, invitandolo anche a sostituirla immediatamente.
- 5) In caso di smarrimento della parola-chiave da parte del legittimo detentore della stessa, provvederà a restituirgli la sua busta e a ricevere subito dopo copia della nuova parola chiave in busta chiusa controfirmata.
- 6) Registrare in un quaderno la data in cui ogni utente cambia la parole-chiave e verificare se ha provveduto alla modifica dopo 6 mesi (3 nel caso che i computer o gli archivi elettronici a cui la parole-chiave dà accesso contengano anche dati sensibili o giudiziari). Eventualmente sollecitarlo al rinnovo. In caso di assegnazione di nuova parole-chiave dal tecnico informatico, verificare che l'Incaricato abbia immediatamente provveduto a inserirne una nuova.
- 7) Ricordare a ogni utente che le parole-chiave devono avere le caratteristiche di cui al punto 5 dell'Allegato B del DLGS 196/2003 (minimo 8 caratteri, evitare nomi, date o altri elementi riferibili all'Incaricato, ecc.)
- 8) Intervenire nel caso che riscontri anomalie o negligenze nella riservatezza della gestione chiavi da parte dei colleghi, richiamandoli cortesemente al corretto comportamento e invitandoli a sostituire immediatamente la parole-chiave che si fosse perduta minando, anche solo potenzialmente, i requisiti di sicurezza.

- 9) Segnalare al Titolare o al Responsabile eventuali problematiche riferibili alla gestione delle parole-chiave.
- 10) Gestire gli eventuali codici di cifratura (se e quando utilizzati) in modo identico a quello descritto per le parole chiave, in modo da assicurarne la disponibilità come previsto nei casi 2) e 3).

Al "Custode" l'istituto metterà a disposizione un cassetta chiudibile a chiave da conservare o in cassaforte o in armadio a chiusura sicura, o altra soluzione equivalente che garantisca un'adeguata condizione di sicurezza. Del contenitore esisteranno soltanto 2 chiavi, date rispettivamente al "Custode" e al suo sostituto.

## PROCEDURA [PRVINFO05] AGGIORNAMENTI DEL SOFTWARE rev. 1.00

Visto il D.Lgs196/2003 art. 31, 33-36 sulle misure minime di sicurezza; Visto il Disciplinare tecnico – allegato B del predetto D.Lgs, in particolare le regole 16, 17, 18, 20, 21, 22, 23 il cui testo si riporta di seguito:

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

Si stabilisce a tal riguardo di nominare un'Incaricato per svolgere detti compiti di aggiornamento del software.

La funzione di "Incaricato degli aggiornamenti del software" prevede i seguenti compiti:

Verificare che siano fedelmente applicati i punti dell'Allegato B sopra citati

Verificare che siano fedelmente eseguite alle scadenze previste le copie di alvataggio e le altre attività descritte nel "DPS", comprese le istruzioni relative al piano di Disaster Recovery e di continuità operativa.

Verificare che siano eseguiti alla giusta cadenza gli aggiornamenti del sistema operativo, dell'antivirus, del firewall, del software in generale.

Verificare che i dischi originali del sistema operativo e di tutti i programmi utilizzati siano presenti e mantenuti in un armadio sicuro, anche in base alle procedure di Disaster Recovery e di continuità operativa.

Ricevere report per la distruzione o formattazione i floppy disk utilizzati, in particolare se contenenti dati sensibili.

In generale monitorare l'evoluzione della situazione e mensilmente riferirne al Titolare al Responsabile.

## PROCEDURA [PRVGEN001] CUSTODIA CHIAVI rev. 1.00

(allegato B del D.Lgs 196/03, regola 29)

Il Disciplinare tecnico – allegato B del D.Lgs 196/03, regola 29, recita:

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

considerato che per garantire una più esatta individuazione dei compiti in materia di sicurezza appare opportuno attribuire alcune specifiche responsabilità;

si è stabilito d'incaricare almeno un Custode delle chiavi dei locali preposti al trattamento.

E' prevista la nomina di uno o più sostituti per casi di assenze.

Il Sostituto/i pertanto avrà una copia delle chiavi in dotazione e si comporterà secondo le stesse istruzioni impartite al Custode.

Si precisa che viene definito archivio ad accesso controllato quell'archivio al quale possono accedere solamente le persone previamente incaricate per iscritto dei trattamenti di dati personali conservati in tale archivio, le quali, inoltre, devono ciascuna volta chiedere la chiave per accedervi e restituirla immediatamente dopo l'uso consegnandola direttamente nelle mani del “Custode”.

Pertanto l'Incaricato dovrà rivolgersi di norma al “Custode” per ricevere la chiave dell'archivio ad accesso controllato. In caso di sua assenza potrà rivolgersi al suo sostituto.

Per le emergenze, copia delle chiavi saranno a disposizione anche del Titolare o di altri da lui delegati, però con le seguenti modalità che assicurino dell'uso esclusivamente per situazioni d'emergenza e della custodia con modalità di elevata sicurezza:

- 1) le chiavi saranno collocate in busta chiusa controfirmata dal “Custode”, munita di opportuna dicitura esterna, e consegnate al DSGA, al Titolare, al sostituto, i quali avranno cura di conservarle in luogo sicuro e le utilizzeranno esclusivamente in caso di assenza del “Custode”.
- 2) Nel caso una busta sia aperta, dovrà essere stilato in un apposito quaderno-registro un breve verbale indicante ora, motivo e autore dell'accesso all'archivio controllato. Il “Custode” provvederà a rimettere la chiave in busta chiusa, mentre il verbale sarà da lui conservato per almeno un anno.
- 3) Il “Custode” terrà la chiave con sé o in luogo sicuro e la consegnerà temporaneamente solamente quando l'Istituto è aperto ed esclusivamente alle persone autorizzate secondo le indicazioni ricevute dal Titolare/Responsabile del trattamento e le regole descritte nel “DPS”.
- 4) Dovrà altresì verificare che le chiavi siano a lui restituite dopo il tempo tecnico strettamente necessario all'accesso all'archivio.

## PROCEDURA [PRVGEN002] ACCESSO AI LOCALI rev. 1.00

I locali preposti ai trattamenti dati sono ad eccesso controllato.

Le porte sono chiuse a chiave e sulle stesse viene affisso un cartello che chiaramente indichi il divieto di accesso.

I Soggetti designati per incarico di trattamento dati, sono responsabili delle attività che si svolgono all'interno di detti locali, di conseguenza è vietato l'accesso al personale non autorizzato.

In casi eccezionali e di provata necessità, è possibile consentire l'accesso ad altri soggetti con le seguenti modalità:

istituire un registro/verbale degli accessi di personale e/o Soggetti diversi dagli Incaricati. Detto registro/verbale riporta:

1. data
2. ora (entrata/uscita)
3. nominativo
4. documento di riconoscimento
5. descrizione di dati e/o documenti a cui ha avuto accesso
6. motivazioni dell'accesso
7. firma

Far compilare il predetto registro al Soggetto che chiede l'accesso ai locali, informandolo che si assume la responsabilità per l'attività che ivi intende svolgere.

Tutte le attività svolte dal soggetto temporaneamente autorizzato, vengono effettuate in presenza di almeno un Incaricato.

A meno di necessità dimostrabili e previa assunzione di responsabilità, nessun documento e/o file (neppure in copia) viene consegnato al Soggetto temporaneamente autorizzato.

## PROCEDURA [PRVINFO03] DIVULGAZIONE E TRASMISSIONE DATI rev. 1.00

I dati riservati e/o sensibili possono essere trasmessi ad altri soggetti purchè si rispetti la seguente regola fondamentale:

*Si verifichi l'esistenza di una previsione di Legge e/o Regolamento che vi obblighi alla trasmissione, ovvero esista esplicito consenso espresso dall'Interessato.*

E' buona prassi che ogni trasmissione sia preceduta e motivata formalmente da parte del richiedente, e che lo stesso indichi, ove esistano, i riferimenti di Legge o Regolamenti.

Se si agisce a fronte di una Legge e/o Regolamento, non è necessario il consenso dell'Interessato, invece obbligatorio in tutti gli altri casi.

La trasmissione e/o divulgazione di dati deve avvenire con certezza di consegna al legittimo destinatario, è quindi buona prassi evitare di utilizzare strumenti che non garantiscono sufficiente grado di segretezza e certezza sulla precisa raggiungibilità.

Si segnalano come poco idonei al tal riguardo strumenti come:

- posta elettronica non certificata (tutta quella tradizionale)
- telefono (voce, sms, mms, ecc.)
- fax
- altri sistemi di trasmissione e messaggistica via web non certificati e criptati

Detti strumenti si possono utilizzare per sollecitare il contatto e/o mettere a conoscenza il legittimo destinatario delle disponibilità (in forma sicura) d'informazioni che lo riguardano.

Si consiglia di utilizzare quale strumenti sicuri:

- la trasmissione scritta in busta chiusa
- la comunicazione verbale in presenza del legittimo destinatario
- la diffusione via web in sessioni ad accesso riservato e criptato

Si ricorda inoltre che per i dati sensibili è necessaria la gestione in forma anonima e disgiunta dai dati anagrafici.

Per la comunicazione scritta sono stati predisposti appositi modelli.

Il destinatario della comunicazione e/o trasmissione s'impegna a rispettare le norme presenti nel Codice della privacy, e si assume ogni responsabilità circa le informazioni/documenti ricevuti.

**PROCEDURA [PRVINFO04] INFORMATIVA EX ART. 13 rev. 1.00**  
(modelli rivolti agl'Interessati, differenziati tra utenza e Personale dell'Istituto)

Sono stati predisposti, messi all'albo e consegnati agl'Interessati, i modelli di informativa ex art. 13 D. Leg.vo 196/03.

Detti modelli sono soggetti a revisione almeno annuale, in accordo con le prerogative di raccolta dati specifiche e dinamiche dell'Istituto.

Sui modelli citati sono chiaramente indicati i criteri:

- definizione della modalità della raccolta dati
- finalità della raccolta dati
- casi di obbligatorietà del consenso
- conseguenze nel caso di mancato rilascio del consenso
- riferimenti del Titolare e del Responsabile

Considerata la specificità della tipologia dati, si è stabilito di adottare 2 modelli d'informativa: il primo rivolto agli Studenti ed alle Famiglie, il secondo rivolto al Personale ed agli altri Soggetti con cui l'Istituto intrattiene rapporti di trattamento dati.

**PROCEDURA [PRVINF005] D.P.S. rev. 1.00**  
(Disciplinare tecnico – All. B D. Legs 196/03, regola 19)

La regola 19 recita:

“Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;”

L'Istituto si è dotato del Documento Programmatico sulla Sicurezza dei dati, per la cui compilazione, si è avvalso della consulenza della società AMBRO SCUOLE S.r.l.

Il D.P.S. è agli atti dell'Istituto ed in copia allegato al presente manuale.

**PROCEDURA [PRVGEN006] esercizio dei DIRITTI DELL'INTERESSATO rev. 1.00**  
(art. 7, D. Leg.vo 196/2003)

Per favorire l'esercizio dei diritti dell'interessato in modo tempestivo e nell'ottica del maggior rispetto dei diritti soggettivi del medesimo, è necessario adottare le seguenti linee guida:

**Procedura per la gestione del diritto di accesso**

01	Gli interessati possono presentare le loro richieste al Titolare o al Responsabile del trattamento;
02	la richiesta può essere presentata direttamente in forma orale o per iscritto, richiedendo l'apposito modulo prestampato messo a disposizione dal Responsabile presso gli uffici di segreteria ovvero a mezzo posta, per fax, per posta elettronica;
03	la richiesta deve essere necessariamente accolta, ai sensi dell'art. 7 del Testo Unico in materia di trattamento dei dati personali, senza che l'interessato debba presentare le proprie motivazioni;
04	unico caso in cui è necessaria la motivazione riguarda l'opposizione per motivi legittimi;
05	la richiesta può provenire anche da una persona fisica diversa dall'interessato o da un'associazione: in questo caso è necessario verificare la delega da parte dell'interessato;
06	la risposta del responsabile alle richieste avanzate deve giungere senza ritardo;
07	si consiglia di rispondere non oltre il termine di tre giorni dal deposito dell'istanza: questo per evitare che l'interessato, dopo cinque giorni, ricorra al Garante per la Privacy;
08	quando è richiesta la comunicazione in forma intellegibile dei dati personali dell'interessato si rileva che può essere effettuata con qualsiasi mezzo: ciò però non deve comportare un facere che la legge non prevede, costringendo l'Istituto scolastico a compiti onerosi, sia in termini di risorse che di tempo.

Il modello per l'esercizio dei diritti ex art. 7, deve essere messo a disposizione degli Interessati anche se non è obbligatoria la compilazione dello stesso. Poter disporre di un formulario compilato, garantisce una migliore comprensione dell'espressione di volontà dell'Interessato e ne circoscrive l'ambito alle sole richieste indicate.