**Istituto Comprensivo "Fracassetti - Capodarco"**
Via Visconti d'Oleggio, 83 / 63900 Fermo
tel: 0734/621273 - fax: 0734/601112
CF: 90055090444 - MECC: APIC841002
sito web: www.iscfracassetticapodarco.gov.it
e-mail: iscfracassetticapodarco@gmail.com
**Istituto a indirizzo musicale**

Prot. n. 176/A03 Fermo, li 10/01/2014

# Regolamento Interno per la Protezione dei Dati

(Documento Programmatico sulla Sicurezza)

## *PREMESSA*

L'Istituto Comprensivo Statale Fracassetti-Capodarco con sede centrale in via Visconti d'Oleggio n.83 - C.F. 90055090444, nella persona del Dirigente Scolastico Ado Evangelisti, C.F. VNGDAO64T15I158F, ha redatto il seguente Documento Programmatico per la Sicurezza ai sensi e per gli effetti dell'art. 34 comma 1, lettera g del D. L.vo n. 196/2003 e del disciplinare tecnico allegato al medesimo sub B "Disciplinare tecnico in materia di misure minime di sicurezza", nonché della "Guida operativa per redigere il documento programmatico" pubblicata sul sito web del Garante.
Scopo del presente documento, di seguito denominato "DPS", è quello di informare l'utenza e i lavoratori delle misure di sicurezza che saranno adottate da questa Istituzione Scolastica relativamente al trattamento dei dati personali

## *Articolo 1: Riferimenti normativi*

Legge 31/12/1996 n. 675 e successive modifiche;
Legge 31/12/1996 n. 676, recante delega al governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
DPR 28/07/1999, n. 318 – Regolamento recante norme per l'individuazione delle misure di sicurezza minime per il trattamento dei dati personali;
Legge 24/03/2001 n. 127, recante delega la governo per l'emanazione di un T. U. in materia di trattamento dei dati personali;
Decreto legislativo 30/06/2003 n. 196 e successive integrazioni e modificazioni – Codice in materia di protezione dei dati personali, in particolare:degli articoli da 28 a 30 (Soggetti che effettuano il trattamento);
degli articoli dal 31 al 36 (Misure di sicurezza);
degli articoli 59 e 60 (Disposizioni relative a specifici settori – Trattamento in ambito pubblico);
degli articoli 95 e 96 (Disposizioni relative a specifici settori – Istruzione);
dell'articolo 180 (Disposizioni transitorie – Misure di sicurezza);
dell'allegato B (Disciplinare tecnico in materia di misure minime di sicurezza);
Per "definizioni" si rispettano quelle riportate all'art. 4 del D.L.vo 196/2003.
D.M. della Pubblica Istruzione n. 305 del 07/12/2006 Regolamento sul trattamento dei dati sensibili e giudiziari nelle scuole;
Legge 06/08/2008 n. 133;
Decreto-Legge "Disposizioni urgenti in materia di semplificazione e sviluppo" del 03/02/2012, n.5 - convertito dalla legge n. 35 del 4 aprile 2012.

## *Articolo 2: Obiettivi del documento*

Il "DPS", redatto in ottemperanza a quanto disposto dal D.L.vo 196/2003 (Codice in materia di protezione dei dati personali) mira a regolamentare e garantire la riservatezza, la sicurezza e la protezione dei dati personali in possesso dell'Istituto Comprensivo Fracassetti-Capodarco, nonché a porre in atto idonee strategie per la protezione delle aree e dei locali interessati a misure di sicurezza. Il Documento garantisce che il trattamento dei dati si svolge nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. Il tutto è disciplinato in modo da assicurare un elevato livello di tutela dei diritti e delle libertà di cui al c. 1 del presente articolo nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte del titolare del trattamento (art. 2 D.L.vo 196/2003). Ai sensi dell'art.1 del D.L.vo: "Chiunque ha diritto alla protezione dei dati personali che lo riguardano".
Tali dati riguardano:

- Il personale che presta servizio presso l'Istituzione Scolastica;
- Gli alunni che frequentano questa Scuola;
- I genitori degli alunni o gli esercenti la potestà familiare per le notizie che trasmettono o portano a scuola;
- I fornitori

In particolare, nel "DPS" vengono definiti i criteri tecnici e organizzativi per:

- la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ad accedere ai medesimi locali;
- i criteri e le procedure per assicurare l'integrità dei dati;
- i criteri e le procedure per la sicurezza della trasmissione dei dati, cartacei o telematici;
- l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi che incombono sui dati e dei modi per prevenire gli eventi dannosi.

## *Articolo 3: Campo di applicazione*

1. Il "DPS" definisce le politiche e gli standard di sicurezza in merito ai dati da garantire e proteggere. Tali dati si distinguono in:
    a. dati personali comuni (dati anagrafici o identificativi delle persone, indirizzi, recapiti telefonici, codici fiscali, dati bancari, informazioni circa la composizione familiare, la professione esercitata da un determinato soggetto, la sua formazione etc.);
    b. dati sensibili (dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute, appartenenza a categorie protette, portatore di handicap, stato di gravidanza, vita sessuale etc.);
    c. dati giudiziari (provvedimenti sul casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reato o dei relativi carichi pendenti, la qualità di imputato o indagato ai sensi degli artt. 60 o 61 del Codice di Procedura Penale, avviso di garanzia, separazioni, affidamento dei figli, etc.).
2. I trattamenti sono realizzati negli uffici di direzione e segreteria, nell'archivio della sede centrale, negli ambienti scolastici ove sono conservati, durante l'anno scolastico, i registri di classe ed i documenti di valutazione degli alunni.
3. I dati sono trattati con fascicoli, atti cartacei e con strumenti elettronici di elaborazione.
4. Il Responsabile e gli Incaricati del trattamento dei dati utilizzano i fascicoli cartacei e i personal computer in dotazione degli uffici.
5. I computer degli uffici di segreteria sono collegati in rete interna e alla rete internet.
6. Gli Incaricati che hanno accesso ad atti e documenti informatici degli uffici sono forniti di password personali e utilizzano codici identificativi. Tali password sono adeguatamente custodite, sulla base delle regole di cui all'Art. 7.

## *Articolo 4: Soggetti che effettuano il trattamento dei dati personali*

Il D.L.vo 196/2003 sulla protezione dei dati personali individua all'art. 4 i soggetti che sono coinvolti nel trattamento dei dati personali:

1. il titolare è la persona fisica e giuridica cui compete la responsabilità finale ed assume decisioni fondamentali riferite alle modalità di trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
2. il responsabile è la persona fisica, dotata di particolari caratteristiche di natura morale e di competenza tecnica, con precise capacità ed affidabilità, preposta dal titolare al trattamento dei dati personali, ivi compreso il profilo della sicurezza;
3. gli incaricati sono le persone fisiche autorizzate a compiere operazioni di trattamento e che materialmente provvedono al trattamento dei dati, secondo le istruzioni impartite dal titolare o dal responsabile;
4. l'amministratore di sistema è il soggetto cui è conferito il compito di "sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base di dati e di consentirne l'utilizzazione". Tale figura è individuata dall' art. 1 del DPR 318/99, mentre non viene riproposta nel D.L.vo 196/2003 che pur conserva una propria funzionalità per la garanzia delle misure di sicurezza logica del sistema informatico della gestione dei dati. Pertanto si ravvisa la necessità di individuare tale figura con delega di compiti definiti.

**1 IL TITOLARE DEL TRATTAMENTO (art. 28 D.L.vo 196/2003)**
Titolare del trattamento, come definito nella Premessa, è il Dirigente Scolastico Ado Evangelisti. E' onere del Titolare del trattamento individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati, che assicurino e garantiscano che vengano adottate le misure di sicurezza. Il Titolare del trattamento affida al Responsabile del trattamento dei dati il compito di adottare le misure tese a ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita dei dati medesimi, anche accidentale, l'accesso non autorizzato o il trattamento non consentito, previe istruzioni fornite per iscritto (art. 31 D.L.vo 196/2003).

**2 IL RESPONSABILE DEL TRATTAMENTO (art. 29 D.L.vo 196/2003)**
In relazione all'attività del Titolare del trattamento, è prevista la nomina di uno o più Responsabili del trattamento, con compiti diversi a seconda delle funzioni svolte. I Responsabili sono individuati tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal Titolare (art. 29 c. 4 D. L.vo 196/03).
**Responsabile del trattamento dei dati: Carla Romagnoli**
Il Titolare del trattamento individua e nomina quale Responsabile del trattamento dei dati il DSGA di questa Istituzione Scolastica, la Signora Carla Romagnoli, persona con inquadramento professionale e ruolo tale da dover fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza.
Il Titolare del trattamento affida a Carla Romagnoli l'onere di individuare, nominare ed indicare per iscritto gli Incaricati del trattamento, mantenendo aggiornato l'elenco delle tipologie dei trattamenti effettuati. Carla Romagnoli ha il dovere di organizzare e gestire la sicurezza dei dati e cartacei, di definire le modalità di accesso ai locali, di definire la gestire delle chiavi di ambienti e scaffali che contengono dati, di informare il Titolare nella eventualità che si siano rilevati dei rischi e di coordinarsi con gli altri Responsabili del trattamento dei dati.
**Responsabile del trattamento dei dati: Sandro Mongardini**
Il Titolare del trattamento individua e nomina quale Responsabile del trattamento dei dati, in relazione ai dati digitali ed al Sistema Informatico, il collaboratore del Dirigente, insegnante Sandro Mongardini, persona con inquadramento professionale, formazione e ruolo tale da dover fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza.
Sandro Mongardini ha il compito di redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi in rete nel dominio SEGETERIA, nonché l'elenco delle tipologie dei trattamenti effettuati; di attribuire ad ogni utente (User) o Incaricato un codice identificativo personale (User-id) per l'utilizzazione dell'elaboratore; di verificare con cadenza almeno semestrale, l'efficacia dei programmi di protezione ed antivirus, nonché di informare il Titolare nella eventualità che si siano rilevati dei rischi. Inoltre a Sandro Mongardini è affidato il compito di gestire e custodire le password per l'utilizzo da parte degli

Uffici delle funzioni Istituzionali sui servizi internet/intranet dei vari Enti o Aziende, come MIUR / INPS / Agenzia delle Entrate / Assicurazione / Banca / INDIRE e tutti gli altri presso quali l'Istituto si accredita telematicamente.
Le password personali per l'accesso ai computer della rete uffici sono gestite direttamente dagli incaricati e dalla Active Directory del Dominio di Windows denominato SEGRETERIA, che impone automaticamente il cambio periodico delle password.
Sandro Mongardini predispone, per ogni incaricato del trattamento, una busta sulla quale è indicato lo USER–ID utilizzato: all'interno della busta deve essere indicata la password utilizzata dall' Incaricato per accedere alla banca-dati. Le singole buste chiuse contenenti le password, timbrate e firmate dal Dirigente, conservate in luogo chiuso e protetto (nell'armadio blindato dell'ufficio del Dirigente). L'apertura delle buste va riportata in apposito verbale conservato assieme alle buste. Le buste vanno sostituite quando l'incaricato modifica periodicamente la propria password.

**Responsabile del trattamento dei dati: Riccardo Agostini**

Il Titolare del trattamento individua e nomina quale Responsabile del trattamento dei dati la Casa Editrice R. Spaggiari S.p.A., in persona del suo rappresentante legale Ing. Riccardo Agostini, l'incarico di Responsabile del trattamento dei dati personali in relazione alle attività di fornitura, aggiornamento e manutenzione degli applicativi gestionali utilizzati per

- la gestione del registro elettronico dell'Istituzione scolastica;
- la gestione, attraverso strumenti elettronici, di servizi di comunicazione e scambio di dati tra la scuola, le famiglie e il personale in servizio. I dati saranno relativi alle attività svolte dall'Istituzione scolastica.

**Responsabile del trattamento dei dati: Lorenzo d'Ortenzi**

Il Titolare del trattamento individua e nomina quale Responsabile del trattamento dei dati la ditta Lorysoft, in persona del suo rappresentante legale Lorenzo d'Ortenzi, l'incarico di Responsabile del trattamento dei dati personali in relazione alle attività di installazione, aggiornamento e manutenzione del dominio di Windows e degli applicativi connessi al supporto tecnico da remoto per le attività di segreteria.

Il Titolare del trattamento dei dati informa i Responsabili dal trattamento dei dati sulle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore mettendo a disposizione sul sito web dell'Istituto una copia delle norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina dei Responsabili del trattamento è a tempo indeterminato, decade per revoca in qualsiasi momento o con il venir meno dei compiti che giustificavano il trattamento.

**3 GLI INCARICATI DEL TRATTAMENTO (art. 30 D.L.vo 196/2003)**

A Carla Romagnoli è affidato il compito di nominare con comunicazione scritta gli Incaricati del trattamento dei dati. La designazione di ciascun Incaricato del trattamento dei dati deve essere effettuata con lettera di incarico in cui sono ben specificati i compiti che gli sono affidati e l'ambito del trattamento consentito.
Gli Incaricati del trattamento devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimento cui sono tenuti.
Agli Incaricati il Responsabile per il trattamento dei dati Sandro Mongardini deve assegnare una parola chiave e un codice identificativo personale.
La nomina degli Incaricati del trattamento deve essere controfirmata dall'interessato per presa visione.

TUTTI I COLLABORATORI SCOLASTICI

Nei loro specifici incarichi o nelle loro mansioni generali previste dal CCNL nell'area specifica di appartenenza (accoglienza e sorveglianza nei confronti degli alunni, ausilio materiale nei confronti degli alunni in situazione di difficoltà, custodia e sorveglianza nei locali scolastici, vigilanza nei confronti del pubblico evitando ed inibendo l'intrusione di persone estranee, collaborazione con i docenti e con il personale di segreteria, pulizia dei locali) osserveranno la massima attenzione alla privacy, evitando di diffondere notizie che devono restare private, in particolare quando ricevono o portano Circolari Ministeriali, Note degli Uffici Superiori o circolari interne in visione ad altro personale, docente e non. Tale personale deve ricevere idonee ed analitiche informazioni da parte del Responsabile del trattamento sulle mansioni loro affidate e sugli adempimenti cui sono tenuti in ragione della riservatezza che si deve per l'incarico affidato e per il fatto di essere dipendenti di questa pubblica istituzione scolastica.
Agli Incaricati del trattamento il Responsabile consegnerà nomina scritta. Tale nomina è a tempo indeterminato, decade per revoca, o con il venir meno dei compiti che giustificavano il trattamento.

AREA DOCENTI
L'unità organizzativa "docenti" è incaricata del trattamento dei dati personali degli alunni necessari allo svolgimento della funzione di istruzione ed assistenza scolastica, anche i docenti esterni incaricati ufficialmente di funzioni nella scuola (esami, corsi, concorsi e attività integrative) entrano a pieno titolo in questa categoria; ogni docente che cessa di far parte di questa unità organizzativa cessa automaticamente dalla funzione di Incaricato, ogni nuovo docente che entra a far parte di questa unità organizzativa assume automaticamente la funzione di incaricato.
I docenti, quali incaricati del trattamento, sono autorizzati a trattare tutti i dati personali con cui entrino comunque in contatto nell'ambito dell'espletamento dell'attività di loro competenza ed in particolare a poter consultare il fascicolo personale degli alunni e qualunque documento necessario per l'attività istituzionale. L'unità organizzativa "docenti" è autorizzata a trattare i dati sensibili e giudiziari con cui i docenti stessi vengano a contatto durante l'attività di loro competenza nell'ambito dell'Istituto; a riguardo viene messo a disposizione questo Regolamento e vengono impartite le seguenti istruzioni generali: il responsabile e gli incaricati devono attenersi rigorosamente a tutte le regole dettate dal D.L.vo 196/2003 e in particolare hanno l'obbligo di mantenere in ogni caso il dovuto riserbo per le informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, anche quando sia venuto meno l'incarico stesso (art. 326 del codice penale e art. 28 della legge 241/90). I docenti e tutte le altre unità di personale che a qualunque titolo hanno rapporto di lavoro anche occasionale (stipule di contratti o convenzioni) con l'Istituzione Scolastica eviteranno di diffondere notizie che resteranno segrete sia per quanto attiene i dati personali, sia per i dati sensibili che hanno acquisito in virtù del loro ufficio. **I docenti non possono estrarre copia di documenti contenenti dati sensibili e giudiziari presenti nel fascicolo degli alunni, potendo tuttavia consultarlo**. Il docente, per la sfera di competenza, rientra nell'ambito degli incaricati sia per le categorie di dati cui può accedere, sia per la tipologia di trattamento e vincoli specifici ai sensi dell'art. 4 del D.L.vo 196/2003, sia per le istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi. I dati trattati dai docenti si rinvengono nei registri dei verbali degli OO.CC., nei registri di classe, dell'insegnante, di modulo per la programmazione, d'intersezione e d'interclasse, nei documenti di valutazione, nelle diagnosi funzionali per la situazione di handicap, nelle assenze degli alunni, in eventuali certificati medici, etc. Il trattamento dei dati da parte dei docenti è definito puntualmente da norme di legge. Tale personale riceverà, nella nomina, specifica informazione/formazione da parte del Titolare del trattamento circa gli specifici doveri e gli adempimenti cui sono tenuti in ragione del loro ufficio, della riservatezza che si deve ai dati che trattano per il fatto di essere dipendenti di questa pubblica istituzione scolastica.

**4 L' AMMINISTRATORE DI SISTEMA (art. 1 DPR 318/99), E GLI INCARICATI DEL BACK-UP**
L'Amministratore di Sistema garantisce la tutela e il corretto uso dei sistemi informatici e delle banche dati in essa contenuti. Dato l'elevato utilizzo delle strumentazioni informatiche, il Titolare del trattamento ritiene opportuno conferire la nomina di Amministratore di Sistema al Primo Collaboratore del Dirigente, Sandro Mongardini in quanto persona idonea, esperta nell'utilizzo dei sistemi informatici e dei relativi programmi, in particolare l'Amministratore di Sistema opera eseguendo le istruzioni fornite dai Responsabili del trattamento dei dati; rispetta le misure di sicurezza previste dalla legge e specificate nel DPS; garantisce la massima riservatezza nel trattamento dei dati; informa tempestivamente il Responsabile di anomalie nel funzionamento del sistema informatico che possono pregiudicare il corretto trattamento dei dati. L'Amministratore di Sistema, in collaborazione con i Responsabili del trattamento dei dati prende tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati; fa in modo che sia prevista la disattivazione dei Codici identificativi personali (User-id). in caso di perdita della qualità, oppure nel caso di mancato utilizzo dei Codici identificativi personali (User-id) per oltre 6 mesi; protegge gli elaboratori dal rischio di intrusione (violazione del sistema) e dal rischio di virus mediante idonei programmi.

Il DSGA e tutti gli Assistenti Amministrativi sono incaricati di eseguire le copie di back-up di documenti utili all'Istituzione scolastica, assicurandosi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro (server di Istituto).

## *Articolo 5: Diritti Dell' Interessato*

L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, come pure l'aggiornamento, la rettifica o, quando vi ha interesse, l'integrazione dei dati. L'interessato ha altresì diritto di richiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge. I dati saranno resi noti solo ai diretti interessati e a persone, enti e organismi che per

legge sono titolati a ricevere i dati stessi. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali (D.L.vo 196/2003). Pertanto per adempiere ai doveri d'ufficio, a disposizioni normative, a precisi obblighi di circolari non si richiede il consenso dell'interessato nell'invio di dati a persone od organismi titolari per legge a ricevere i dati stessi. I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato.

## *Articolo 6: Analisi dei rischi che incombono sui dati*

1. Le situazioni dei rischi che incombono sui dati possono riguardare:
   - Dati su materiale cartaceo;
   - Dati su attrezzature informatiche;
   - I luoghi e i contenitori che custodiscono sia i materiali cartacei, sia le attrezzature informatiche.

2. I materiali cartacei a rischio sono:
   - Raccoglitori e faldoni che raccolgono i documenti contenuti nei fascicoli del personale;
   - Schede personali degli alunni;
   - Registri (di classe, di modulo, di presenza);
   - Registro dello stato del personale;
   - Decreti e certificati sulle persone;
   - Anagrafe fornitori;
   - Contratti e convenzioni;
   - Documentazione finanziaria e contabile;
   - Registro infortuni;
   - Moduli di iscrizione, istanze, etc
   - Atti affissi agli albi.

3. I dati informatici a rischio sono quelli contenuti nei documenti di cui al comma 2 del presente articolo e immessi nei personal computer degli uffici.

4. Gli eventi che possono generare danni e che comportano rischi per la sicurezza dei dati personali si distinguono sotto un triplice aspetto:
   - Comportamento degli operatori:
     i. Sottrazioni di credenziali di autenticazione;
     ii. Carenza di consapevolezza, disattenzione o incuria;
     iii. Manomissioni e comportamenti sleali o fraudolenti;
     iv. Errore materiale;
   - Eventi relativi agli strumenti:
     i. Azione di virus informatici o di programmi suscettibili di recare danno;
     ii. Malfunzionamento, indisponibilità o degrado degli strumenti;
     iii. Guasto ai sistemi complementari ( impianto elettrico, gruppo di continuità, climatizzazione, etc.).
   - Eventi relativi al contesto fisico-ambientale:
     i. Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, etc.), nonché dolosi, accidentali o dovuti ad incuria;
     ii. Accesso di estranei o persone non titolari di incarichi e responsabilità nel trattamento dei dati;
     iii. Errori umani nella gestione della sicurezza fisica.
     iv. Accessi esterni non autorizzati;
     v. Vandalismo;
     vi. Intercettazioni di informazioni in rete;
     vii. Spamming, tecnica di sabotaggio o posta spazzatura: vettore attraverso il quale si fanno circolare virus e codici maligni di ogni tipo con l'obiettivo di compromettere il funzionamento dei computer a catena e rendere al contempo più difficile il tracking, cioè l'individuazione da parte delle forze di polizia preposte al compito di garantire la sicurezza della società dell'informazione, ma è altresì piaga planetaria e veicolo per vendere software contraffatti, in una sorte di e-commerce illegale;
     viii. Sottrazione di strumenti contenenti dati;

## *Articolo 7: Misure da adottare per garantire l'integrità e la disponibilità dei dati e la protezione delle aree e dei locali*

**1. MISURE DA ADOTTARE**

Al fine di garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia ed accessibilità, sono state adottate le seguenti misure:

- Individuazione e nomina del Responsabile del trattamento dei dati per garantire tutte le misure di sicurezza per la conservazione e utilizzazione dei dati
- Misure di prevenzione per eliminare gli eventuali incendi con adeguate modalità di gestione degli stessi;
- Individuazione dei locali e contenitori (armadi, armadi di sicurezza, armadi blindati, classificatori con serrature, apparecchiature e strumenti di raccolta dei dati adeguati e sicuri, etc.);
- Regolamentazione sia per il personale che per gli esterni nell'accesso ai locali e alle attrezzature che conservano dati, archivi e documentazione,
- Attuazione di misure di protezione attiva e passiva dei locali;
- Salvataggio automatico dei dati su server. Periodico salvataggio manuale dei dati del server su unità rimovibili.
- Verifica periodica (almeno ogni tre mesi) della funzionalità e dell'efficienza delle misure di protezione e delle strutture.
- Installazione di antivirus sul server e sui client con gestione centralizzata degli allarmi e degli aggiornamenti, al fine di impedire l'attacco di virus, ingressi non autorizzati, intercettazioni sulla rete informatica.

**2. CRITERI, PROCEDURE PER GARANTIRE L'INTEGRITA' DEI DATI**

Il Responsabile del trattamento, con il supporto dell' Amministratore di Sistema, stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati.
In particolare per ogni banca di dati devono essere definite le seguenti specifiche:

- tipo di supporto da utilizzare per le copie di back-up;
- numero di copie di back-up da effettuare;
- tempi e scadenze e modalità per effettuare le copie di back-up;
- stima della durata massima di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati;
- assegnazione periodica del compito di effettuare le copie di back-up agli Incaricati del trattamento.

Il Sistema informatico installato presso l'Istituto semplifica il lavoro del personale degli uffici, in quanto prevede il back-up automatico sul server d'Istituto dei file presenti nelle cartelle "Desktop" e "Documenti" di tutti i computer degli uffici, oltre al back-up della posta elettronica istituzionale, certificata e non.
Gli utenti devono provvedere personalmente al back-up di file o impostazioni che non siano contenute in una delle due cartelle sopra menzionate, anche se l'uso di altre cartelle è sconsigliato.

L'Amministratore di Sistema deve effettuare ogni 6 mesi una copia di back-up di tutti i dati su supporto esterno (es. DVD), verificare che tale copia sia integra e leggibile e conservarla nella cassaforte del Plesso della scuola secondaria Fracassetti, che è un altro edificio rispetto a quello degli uffici.

L'accesso ai supporti utilizzati per il back-up dei dati è limitato:

- Al Titolare del trattamento;
- Ai Responsabili del trattamento della sicurezza dei dati Carla Romagnoli e Sandro Mongardini;
- All'Amministratore di Sistema Sandro Mongardini.

Quando il Responsabile del trattamento, in sintonia con l' Amministratore di Sistema, decide che i supporti utilizzati per le copie di back-up delle banche-dati non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a distruggerli e/o a farne cancellare il contenuto annullando le informazioni in esso contenute.

**3. PROTEZIONE DA VIRUS INFORMATICI**

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita degli stessi a causa di virus informatici, il Responsabile del trattamento dei dati Sandro Mongardini stabilisce quali protezioni software

adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato. Il Responsabile del trattamento stabilisce inoltre la periodicità, con cui devono essere effettuati gli aggiornamenti dei sistemi antivirus utilizzati per ottenere un accettabile standard di sicurezza dei dati trattati Gli Incaricati che utilizzano i sistemi informatici annotano gli eventuali virus rilevati, e, la fonte da cui sono pervenuti, al fine di isolare o comunque trattare con precauzione i possibili portatori di infezioni informatiche. Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezioni o contagio da virus, il Responsabile del trattamento / Amministratore di Sistema, deve provvedere a: isolare il sistema, verificare se ci sono altri sistemi infettati con lo stesso virus informatico, identificare l'antivirus adatto e bonificare il sistema infetto, installare l'antivirus adatto su tutti i sistemi, compilare un modulo di "Report dei contagi da virus informatici", da conservare a cura del Responsabile del trattamento.

## 4. PROTEZIONE DELLE AREE, DEI LOCALI E DEGLI ARMADI

### Sicurezza di area

Gli interventi per la sicurezza di area servono per prevenire accessi fisici non autorizzati, danni o interferenze nello svolgimento dei servizi. Le misure si riferiscono alla protezione perimetrale dei siti, ai controlli fisici all'accesso, alla sicurezza degli archivi e delle attrezzature informatiche rispetto ai danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.

Nessuno accede all'archivio se non autorizzato, i fascicoli prelevati dall'archivio permangono al di fuori del sito per il tempo strettamente necessario e successivamente vengono riposti al proprio posto. Gli incaricati accedono ai dati personali la cui conoscenza sia strettamente necessaria per evadere una pratica, i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento devono essere conservati e custoditi con le necessarie precauzioni.

Ciascun incaricato, conoscendo le mansioni di ufficio cui è stato assegnato, avrà indicazioni sui locali, scaffali, armadi e documenti cui può accedere. Nel caso in cui i locali, gli scaffali e gli armadi siano provvisti di chiave, ciascun incaricato che vi può accedere avrà in consegna le chiavi per aprire e chiudere. Le chiavi devono essere conservate da ciascun incaricato con la massima attenzione, in modo tale che nessuno non autorizzato possa accedere a locali o armadi chiusi senza effrazione.

Una copia di tutte le chiavi sarà mantenuta nell'armadio blindato della presidenza. Le chiavi dell'armadio blindato saranno duplicate in sole due copie, una in consegna al Dirigente e l'altra in consegna al DSGA in busta chiusa timbrata e firmata dal Dirigente.

## 5. GESTIONE DELLE PASSWORD PERSONALI PER L'ACCESSO ALLA RETE DEGLI UFFICI

La rete di computer degli Uffici dell'Istituto è configurata in modo tale che ciascun utente abbia una password personale per accedere al computer.

Qualificandosi con il proprio account (nome utente e password) ciascun utente può accedere ai propri dati salvati nelle cartelle "Documenti" e "Desktop" da uno qualsiasi dei computer degli uffici. Si ricorda che tali dati restano salvati anche sul server, quindi anche in caso di rottura del disco o del computer personali possono essere recuperati.

Oltre a questa esistono, per la gestione di tutte le pratiche d'ufficio, altre password personali, che consentono all'utente di identificarsi presso altri servizi, come ad esempio la password personale di accesso al SIDI.

Le password personali non devono essere comunicate ad alcuno, né trascritte su agende/fogli di carta/post-it/file/ecc. che possano essere letti da altri. Qualsiasi gestione diversa delle password personali deve risultare da atto scritto e motivato, firmato dal Dirigente.

## 6. GESTIONE DELLE PASSWORD ISTITUZIONALI

Per motivi di lavoro gli Assistenti Amministrativi possono avere a disposizione password istituzionali per accedere a servizi di vari Enti o Aziende: MIUR / INPS / Agenzia delle Entrate / Assicurazione / Banca / INDIRE e molti altri.

Tali password non devono essere comunicate ad alcuno, né trascritte su agende/fogli di carta/post-it/file/ecc. che possano essere letti da altri.

Una copia di TUTTE le password istituzionali che vengono assegnate all'Istituto va conservata in un apposito registro, nella cassaforte della Dirigenza. In caso sia necessario recuperarla, il permesso andrà richiesto al Dirigente.

Qualsiasi assegnazione / modifica di password Istituzionali deve essere segnalata al Dirigente e conservata nel registro di cui sopra.

## *Articolo 8: Criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento*

In caso di danneggiamenti, smarrimenti, inaffidabilità della base dati:

- per i dati cartacei si potrà ricostruire copia da documenti e atti in possesso degli interessati (personale in genere) o di altri enti cui sono stati trasmessi (Scuole, MIUR, Ufficio Scolastico Regionale, USP, ASL, Comune, ecc.);
- per i dati informatici si potranno ricostruire i dati danneggiati ricavando gli stessi dalle copie di back-up o, in subordine, da atti e documenti "stampati" cartacei.

Il Responsabile del trattamento Sandro Mongardini ha il compito di verificare almeno ogni sei mesi la situazione dei Sistemi operativi installati sulle apparecchiature con le quali vengono trattati i dati. La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi, per quanto riguarda: la sicurezza dei dati trattati, il rischio di distruzione o di perdita dei dati, il rischio di accesso non autorizzato o non consentito.
Nel caso esistano evidenti rischi sui Sistemi operativi, l'Amministratore di sistema / il Responsabile Sandro Mongardini informa il Titolare perché siano presi gli opportuni provvedimenti alla scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore ad evitare che possano essere smarriti, danneggiarti o distrutti.

## *Articolo 9: Interventi formativi per gli incaricati del trattamento*

Ai Responsabili del trattamento dei dati Carla Romagnoli e Sandro Mongardini è affidato il compito di verificare ogni anno i bisogni formativi di cui necessitano gli Incaricati, specie per le innovazioni nel campo informatico.
E' necessario tenere il personale continuamente informato e all'altezza dei compiti che deve espletare, per meglio conoscere i rischi che incombono sui dati, per avere una ottimale conoscenza delle misure di sicurezza e degli adeguati comportamenti da adottare, delle responsabilità circa i dati danneggiati, persi o distrutti.
Gli interventi formativi sono particolarmente opportuni al momento dell'ingresso in servizio di personale nuovo, per immissione in ruolo o per trasferimento, in occasione dell'adozione di nuovi strumenti o dell'installazione di altri software. E' opportuno documentare gli interventi formativi. Le varie tipologie di corsi di formazione potranno essere effettuati singolarmente da questa Istituzione Scolastica o in rete con altre Scuole.
E' messo a disposizione del personale, sul sito d'Istituto www.iscfracassetticapodarco.gov.it il D. L vo 196/2003.

## *Articolo 10: Norme finali*

Questo Regolamento potrà essere integrato e aggiornato in qualunque periodo dell'anno. Per quanto non regolamentato nel presente documento, si applicano le norme contenute nel D.L.vo 196/2003 e dallo stesso richiamate.
Il D.S. titolare del trattamento dei dati si impegna ad adottare, nella fase di graduale attuazione degli interventi previsti dalla normativa sulla tutela della privacy, ogni possibile misura destinata a salvaguardare la sicurezza dei dati personali, siano essi contenuti nei documenti cartacei che registrati mediante strumenti elettronici.
Tali misure riguarderanno gli aspetti organizzativi, logistici e procedurali miranti ad evitare con ogni mezzo qualsiasi incremento di rischi di distruzione o perdita, anche accidentale, dei dati oggetto di trattamento, di accesso non autorizzato o di trattamento non consentito.

Il Titolare del trattamento dei dati
Dirigente
Ado Evangelisti