



ISTITUTO COMPRENSIVO “G. PASCOLI”
di Scuola dell’Infanzia, Primaria e Secondaria di I Grado
P.za Paolo Ercole, 6 – 15023 Felizzano (AL) - CF96034370062
Tel.0131-791122 – sel. 2 – FAX 0131-791395

www.icpascoli-felizzano.gov.it

email: icpascoli-felizzano@libero.it – alic81800q@istruzione.it – PEC: alic81800q@pec.istruzione.it

Prot. n. 930/A2

Felizzano, 31.03.2015

P R I V A C Y

(D.L.vo N. 196/2003)

DISPOSIZIONI MINIME SULLA SICUREZZA

E

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

PREMESSA

Scopo di questo documento è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi in materia di sicurezza del trattamento dei dati effettuato dall' **Istituto Comprensivo "G.Pascoli" - Felizzano** previsti dal D.L.vo 30/06/2003 "Codice in materia di protezione dei dati personali".

Atteso che la suddetta Istituzione Scolastica è tenuta a prevedere ed applicare le misure minime di sicurezza di cui agli artt.31 e ss. del D.L.vo n.196/2003, essa adotta il presente documento programmatico della sicurezza.

Articolo 1

NORMATIVA DI RIFERIMENTO

- D.L.vo n. 196 del 30/06/2003;
- Regolamento interno per l'utilizzo della rete.

Articolo 2

DEFINIZIONI E RESPONSABILITÀ

AMMINISTRATORE DI SISTEMA: il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. In questo contesto l'amministratore di sistema assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali.

Ai fini della sicurezza l'amministratore di sistema ha le responsabilità indicate nella lettera di incarico.

CUSTODE DELLE PASSWORD: il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.

DATI ANONIMI: i dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

DATI PERSONALI: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

DATI IDENTIFICATIVI: i dati personali che permettono l'identificazione diretta dell'interessato.

DATI SENSIBILI: i 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 e la vita sessuale.

DATI GIUDIZIARI: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del codice di proc. penale.

TRATTAMENTO: qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, anche se non registrati in una banca dati.

INCARICATO: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate nella lettera di incarico.

INTERESSATO: il soggetto al quale si riferiscono i dati personali.

RESPONSABILE DEL TRATTAMENTO: il soggetto preposto dal titolare al trattamento dei dati personali. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.

RESPONSABILE DELLA SICUREZZA INFORMATICA: il soggetto preposto dal titolare alla gestione della sicurezza informatica. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza il responsabile del sistema informativo ha le responsabilità indicate nella lettera di incarico.

TITOLARE: il titolare del trattamento è l'Ente (ISTITUTO SCOLASTICO) e la titolarità è esercitata dal rappresentante legale (DIRIGENTE SCOLASTICO), tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

Articolo 3

TRATTAMENTO E NATURA DEI DATI

L'Istituzione scolastica tratta dati personali (comuni, sensibili, giudiziari) di studenti, genitori, personale dipendente, fornitori, esperti esterni.

I trattamenti sono effettuati sia con modalità manuali e/o con l'ausilio di strumenti elettronici o comunque automatizzati per le seguenti finalità:

- Adempimenti agli obblighi di fonte legislativa, nazionale o comunitaria, regolamentare o derivante da atti amministrativi
- Somministrazione dei servizi formativi
- Gestione del personale docente e non docente
- Formazione degli alunni, del personale docente e non docente
- Adempimenti assicurativi
- Tenuta della contabilità

Articolo 4
TITOLARE, RESPONSABILI, INCARICATI

Titolare del trattamento: **DIRIGENTE SCOLASTICO**

Responsabile del trattamento dei dati: **DSGA**

Responsabile della sicurezza informatica: **DSGA**

Amministratore della rete: **INFORMATICA SERVICE**

Custode delle password: **ASS.TE AMM.VO**

Incaricati del trattamento dei dati: come da allegato 1

INFORMATICA SERVICE S.r.l.
Via Ghilini 10 -15100 Alessandria
Tel. 0131/444555

Articolo 5
ANALISI DEI RISCHI

L'analisi dei rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo e avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.

L'analisi dei rischi consiste nella:

- individuazione di tutte le risorse del patrimonio informativo;
- identificazione delle minacce a cui tali risorse sono sottoposte;
- identificazione delle vulnerabilità;
- definizione delle relative contromisure.

La classificazione dei dati in funzione dell'analisi dei rischi risulta la seguente:

- DATI ANONIMI, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI,
 - DATI PERSONALI SEMPLICI, ovvero la classe di dati a rischio intermedio
 - DATI PERSONALI SENSIBILI/GIUDIZIARI, ovvero la classe di dati ad alto rischio;
 - DATI PERSONALI SANITARI, ovvero la classe di dati a rischio altissimo.

Articolo 6
INDIVIDUAZIONE DELLE RISORSE DA PROTEGGERE

Le risorse da proteggere sono:

- personale;
- dati/informazioni;
- documenti cartacei;
- hardware;
- software;
- apparecchiature di comunicazione;
- manufatti vari;
- servizi;
- apparecchiature per l'ambiente;
- immagine della scuola.

Articolo 7
INDIVIDUAZIONE DELLE MINACCE

Dalla ricognizione dei rischi che potrebbero comportare una distruzione, sottrazione, perdita, trattamento abusivo dei dati, di origine dolosa, colposa, ovvero meramente fortuito, in grado di recare pregiudizio ai dati personali trattati, sono state individuate le seguenti fonti di rischio:

- a) **COMPORAMENTI DEGLI OPERATORI**
 - I. Sottrazione di credenziali di autenticazione
 - II. Comportamenti imperiti, imprudenti o negligenti
 - III. Comportamenti dolosi
 - IV. Errori materiali

- b) **EVENTI RELATIVI AGLI STRUMENTI**
 - I. Virus informatici
 - II. Malfunzionamento, indisponibilità o usura fisica degli strumenti
 - III. Accessi abusivi
 - IV. Intercettazione dei dati durante le trasmissioni in rete

- c) **EVENTI RELATIVI AL CONTESTO FISICO – AMBIENTALE**
 - I. Distruzione o perdita di dati a causa di eventi incontrollabili ovvero, seppur teoricamente prevedibili, di origine fortuita, dolosa o colposa, per i quali non è possibile apprestare cautele
 - II. Guasti a sistemi complementari
 - III. Furto o danneggiamento degli strumenti elettronici
 - IV. Accesso non autorizzato da parte di terzi
 - V. Errori umani nell'attuazione degli strumenti di protezione

In particolare, nella tabella seguente sono elencati eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse indicate all'articolo 6 con la valutazione della classe di gravità del rischio, tenendo conto della concreta possibilità di realizzazione presso l'Istituzione scolastica.

Allo scopo è stata adottata la seguente scansione:

EE= MOLTO ELEVATO A= ALTO MA=MEDIO M=MEDIO MB=MEDIO-BASSO
B=BASSO

Rischi	Deliberato	Accidentale	Ambientale
Terremoto			M
Inondazione			MA
Temporale– tempesta – tromba d'aria			MB
Fulmine	B	MB	
Fuoco	B	MB	
Danno volontario	B		
Interruzione di corrente		M	
Interruzione di acqua		M	
Guasto hardware	B	M	
Linea elettrica instabile		M	M
Temperatura e umidità eccessive			B
Polvere			MB
Radiazioni elettromagnetiche		B	
Scariche elettrostatiche		B	
Furto	B		

Uso non autorizzato dei supporti di memoria	B		
Deterioramento dei supporti di memoria		M	
Errore del personale operativo		M	
Errore di manutenzione		M	
Masquerading dell'identificativo dell'utente	M		
Uso illegale di software	B	M	
Software dannoso		M	
Esportazione/importazione illegale di software	B		
Accesso non autorizzato alla rete	B		
Uso della rete in modo non autorizzato	B		
Guasto tecnico di provider di rete		M	
Danni sulle linee	B	MA	
Errore di trasmissione		M	
Sovraccarico di traffico	B	MA	
Intercettazione (Eavesdropping)	B	M	
Infiltrazione nelle comunicazioni	B	M	
Analisi del traffico		M	
Indirizzamento non corretto dei messaggi	B	M	
Reindirizzamento dei messaggi	B		
Guasto dei servizi di comunicazione	MB	M	
Mancanza di personale		M	
Errore dell'utente	B	M	
Uso non corretto delle risorse	MB	M	
Guasto software	B	M	
Uso di software da parte di utenti non autorizzati	MB	MB	
Uso di software in situazioni non autorizzate	MB	MB	

Articolo 8 **INDIVIDUAZIONE DELLE VULNERABILITÀ**

Nelle tabelle seguenti sono elencate le vulnerabilità del sistema informativo che possono essere potenzialmente sfruttate qualora si realizzasse una delle minacce indicate nell'articolo 7.

Infrastruttura	Hardware	Comunicazioni
Mancanza di protezione fisica dell'edificio (porte finestre ecc.)	Mancanza di sistemi di rimpiazzo	Linee di comunicazione non protette
	Suscettibilità a variazioni di tensione	Giunzioni non protette

Linea elettrica instabile	Suscettibilità a variazioni di temperatura	Mancanza di autenticazione
	Suscettibilità a umidità, polvere, sporcizia	Trasmissione password in chiaro
	Suscettibilità a radiazioni elettromagnetiche	Mancanza di prova di ricezione/invio
	Manutenzione non sempre adeguata	
	Controllo saltuario delle configurazioni (update/upgrade dei sistemi)	Traffico sensibile non protetto
		Gestione non sempre adeguata della rete

Documenti cartacei	Software	Personale
Locali documenti abbastanza non protetti	Interfaccia uomo-macchina complicata	Carenza di personale adeguatamente formato e da formare al proposito
Non sempre adeguate precauzioni nell'eliminazione	Mancanza di identificazione / autenticazione	Carenza di supervisione di specialisti esterni
Sufficiente controllo delle copie	Mancanza del registro delle attività (log)	Formazione accettabile sulla sicurezza
	Errori noti del software	Scarsa consapevolezza
	Tabelle di password non protette	Uso non sempre corretto di hardware/software
	Carenza di password management	Carenza di monitoraggio
	Appena sufficiente allocazione dei diritti di accesso	Procedure di reclutamento inadeguate rispetto alle esigenze
	Appena sufficiente il controllo nel caricamento e uso di software	
	Carenza di controllo di configurazione	
	Carenza di documentazione	

Articolo 9

INDIVIDUAZIONE DELLE CONTROMISURE

Le contromisure individuano le azioni che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce, esse sono classificabili nelle seguenti tre categorie:

- contromisure di carattere fisico;
- contromisure di carattere procedurale;
- contromisure di carattere elettronico/informatico.

Nota generale:

Presenza di sistema di allarme nelle porte principali di ingresso dell'Istituto, uso di lucchetti e serrature alle porte delle stanze nelle quali sono allocate postazioni informatiche pur essendo l'edificio della scuola ottocentesco, pur in presenza di infissi d'epoca non sempre a tenuta totale, le imposte interne vengono chiuse e finestre e porte accuratamente chiuse con le serrature disponibili. Più volte è stato richiesto l'intervento dell'Amministrazione Comunale per adeguare le contromisure di carattere fisico anti effrazione a uno standard più elevato e sicuro.

Contromisure di carattere fisico

il locale di segreteria ad accesso pubblico risulta separato dall'area ad accesso controllato per mezzo di una struttura (mobili da ufficio) adeguatamente posizionata;

- le apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati personali o sensibili/giudiziari e apparecchiature di telecomunicazione, dispositivi di copia) e gli archivi cartacei contenenti dati personali o sensibili/giudiziari sono situati in locali ad accesso controllato e custoditi in mobili archivio muniti di serratura;
- i locali ad accesso controllato sono all'interno di aree sotto la responsabilità dell'Istituto Comprensivo "G.Pascoli" di Felizzano;
- i responsabili dei trattamenti indicati nell'allegato 1 sono anche responsabili dell'area in cui si trovano i trattamenti;
- i locali ad accesso controllato sono chiusi.
- l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area sotto la responsabilità dell'Istituto Comprensivo "G.Pascoli" di Felizzano;
- i locali adibiti a segreteria non sono provvisti di estintori ma l'estintore si trova comunque nel corridoio adiacente alle segreterie;
- sono state segnalate le necessità di interventi atti a dotare i locali ad accesso controllato di estintori adeguati anche per le dotazioni informatiche;
- verrà inoltre richiesta l'installazione di un estintore a polvere nel laboratorio di informatica; si fa presente che negli immediati pressi è allocata una sistrada anti incendio e un estintore nel corridoio.

Contromisure di carattere procedurale

- l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate;
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- i visitatori abituali sono ammessi all'area ad accesso controllato solo se accompagnati da persone autorizzate;
- i visitatori occasionali delle aree ad accesso controllato devono essere accompagnati da un incaricato;
- è controllata l'attuazione del piano di verifica periodica sull'efficacia degli estintori;
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento di tali dati;
- i registri di classe, contenenti dati comuni e particolari, durante l'orario delle lezioni devono essere tenuti in classe sulla scrivania e/o affidati all'insegnante di turno; al termine delle lezioni vengono depositati dall'insegnante dell'ultima ora di lezione in Presidenza in un armadio chiuso a chiave;
- il docente è responsabile della riservatezza del registro personale in cui sono annotati dati comuni e particolari; fuori dall'orario di servizio il registro viene conservato nell'armadietto del docente che è chiuso a chiave;
- ogni docente è custode e responsabile della password di accesso personale al registro elettronico (applicativo RES della Ditta Spaggiari);
- il protocollo riservato, accessibile solo al Titolare e al Responsabile del trattamento è conservato in Presidenza in un armadio chiuso a chiave;
- per il trattamento dei soli dati cartacei sono adottate le seguenti disposizioni:
 - si accede ai soli dati strettamente necessari allo svolgimento delle proprie mansioni;
 - si utilizzano archivi con accesso selezionato;

- atti e documenti devono essere restituiti al termine delle operazioni;
- è fatto divieto di fotocopiare/scannerizzare documenti senza l'autorizzazione del responsabile del trattamento;
- è fatto divieto di esportare documenti o copie dei medesimi all'esterno dell'Istituto senza l'autorizzazione del responsabile del trattamento, tale divieto si estende anche all'esportazione telematica;
- il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti deve essere ridotto in minuti frammenti.

Contromisure di carattere elettronico/informatico

Vedere l'Allegato.

Articolo 10 ***NORME PER IL PERSONALE***

Tutti i dipendenti concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa e indicate nell'articolo 6 , nel rispetto di quanto stabilito nel presente documento e dal regolamento di utilizzo della rete.

Articolo 11 ***INCIDENT RESPONSE E RIPRISTINO***

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, è stata definita una procedura di periodica esecuzione di copie di sicurezza dei dati trattati. I documenti sono conservati in copia cartacea presso i locali dell'Istituto non accessibili a terzi e dotati di adeguati strumenti di protezione.

Articolo 12 ***PIANO DI FORMAZIONE***

La formazione degli incaricati viene effettuata all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati. Le finalità della formazione sono:

- sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali;
- proporre buone pratiche di utilizzo sicuro della rete;
- riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza.

L'Istituzione scolastica aderisce alle iniziative formative organizzate dall'Ufficio Scolastico Regionale, tenendo anche conto della economicità di una azione organizzata su base regionale.

E' prevista in ogni caso un'attività di formazione ed autoformazione di complessive 4 ore all'inizio di ogni anno scolastico per tutto il personale incaricato di trattamento dei dati.

Questo Istituto ha aderito, tra l'altro, alla "Proposta attività di formazione prevista dal d.lgs. 196/2003 in materia di protezione dei dati personali" prot. n. 10853/P/A21 Circ.Reg.n.339 del 07/10/2005 USR-Piemonte; l'intervento formativo è stato rivolto ai responsabili e incaricati della sicurezza dei dati delle Istituzioni Scolastiche e degli Uffici Amministrativi.

Articolo 13 ***AGGIORNAMENTO DEL PIANO***

Il piano deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:

- modifiche all'assetto organizzativo della scuola ed in particolare del sistema informativo (sostituzioni di hardware, software, procedure, connessioni di reti, ecc.) tali da giustificare una revisione del piano;
- danneggiamento o attacchi al patrimonio informativo della scuola tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.

ELENCO ALLEGATI COSTITUENTI PARTE INTEGRANTE DI QUESTO DOCUMENTO

- Allegato 1 - elenco trattamenti dei dati
- Allegato 2 - minacce hardware, minacce rete, minacce dati trattati, minacce supporti
- Allegato 3 - misure di carattere elettronico/informatico, politiche di sicurezza, incident response e ripristino
- Allegato 4 - regolamento per l'utilizzo della rete in segreteria e in direzione.
- Allegato 5 – uso del proxy
- Informativa per il trattamento dei dati personali degli alunni e delle loro famiglie
- Informativa per il trattamento dei dati del personale dipendente
- Informativa per il trattamento dei dati delle aziende fornitrici e degli enti e associazioni che hanno rapporti con la scuola
- Informativa gestione sito web
- Lettere di incarico per il Responsabile del trattamento dei dati
- Lettera di incarico per il Custode delle password
- Lettere di incarico per l'Amministratore di sistema
- Lettere di incarico per il trattamento dei dati: unità organizzativa “Docenti”
- Lettere di incarico per il trattamento dei dati: personale di Segreteria
- Lettere di incarico per il trattamento dei dati: Collaboratori Scolastici
- Modello “Riservatezza” per e-mail in uscita

Gli allegati al presente documento ne fanno parte integrante.

Il presente Documento Programmatico sulla Sicurezza deve essere divulgato e illustrato a tutti gli incaricati.

Copia del medesimo è affissa all'Albo dell'Istituto.

Felizzano,

Il Titolare del trattamento
Il Dirigente Scolastico
(*dott.ssa Maria Paola MINETTI*)

Nota: Fonti di documentazione

Il modello di documento programmatico sulla sicurezza è stato predisposto consultando le seguenti fonti:

- <http://www.garanteprivacy.it>
- <http://www.osservatoriotecnologico.net>
- “Sicurezza informatica” ECDL IT Administrator – Modulo 5 Testo di riferimento per la certificazione EUCIP - McGraw Hill ISBN 88-3864333-4 Tabelle Minacce e vulnerabilità Cap. 1
- Il regolamento per l'utilizzo della rete è stato derivato dal documento proposto alla Giornata di studio CISEL 0203G286 – CISEL Centro Studi per gli Enti Locali – Maggioli



ISTITUTO COMPRENSIVO “G. PASCOLI”
di Scuola dell’Infanzia, Primaria e Secondaria di I Grado
P.zza Paolo Ercole, 6 – 15023 Felizzano (AL) - CF96034370062
Tel.0131-791122 sel. 2 – FAX 0131-791395

www.icpascoli-felizzano.gov.it

email: icpascoli-felizzano@libero.it – alic81800q@istruzione.it – PEC : alic81800q@pec.istruzione.it

Documento programmatico sulla sicurezza (ai sensi del D.L.vo n.196 del 30/06/2003)

ALLEGATO 3 – Misure, incident response, ripristino

Tabella 1 - Connettività internet

Logistica	Connettività	Apparecchiature di comunicazione	Provider
Direzione	ADSL	Modem	Libero.it/istruzione.it
Segreteria	ADSL	Modem	Libero.it/istruzione.it

Logistica: ubicazione postazione connessa

Connettività: tipo di connettività internet (XDSL, ISDN, PSTN) utilizzata.

Apparecchiature di comunicazione: tipo di apparecchiature utilizzate per la connettività (modem, router).

Provider: fornitore di connettività (MIUR, RUPAR, altro).

Tabella 2 - Descrizione Personal Computer¹

Identificativo del PC	Tipo PC	Sistema operativo	Rete	Software utilizzato	Assegnato a:
Work 1	ACER VERITON X2610 G INTEL PENTIUM CPUG640	Windows 7	Si	OFFICE SISSI	Viotti Anna
Work 20	HP PRO 3010 MICROTOWER PC	Wind. XP Professional Versione 2002	Si	OFFICE SISSI	Palla Riccardo
Work 3	HP PRO 3515 AMD A4 5300 APU	Windows 7	Si	OFFICE SISSI	Lanzavecchia Carla
Work 4	HP PRO 3010 MICROTOWER PC	Wind. XP Professional Versione 2002	Si	OFFICE SISSI	Messoriano Maria Teresa
Work 7	ACER VERITON X2610 G INTEL PENTIUM CPUG640	Windows 7	Si	OFFICE SISSI	Migliardi Franca
Work 8	HP PRO 3515 AMD A4 5300 APU	Windows 7	Si	OFFICE SISSI	Milioto Giovanna
PC Server	HP PROLIANT ML 110 GT	Windows SERVER 2008	Si	SISSI WINDO WS 2008	UNITA' CENTRALE ⁽¹⁾

Identificativo del PC: elenco di tutti i PC utilizzati sia connessi che non connessi alla rete

Tipo PC: tipo del PC.

Sistema operativo: Sistema operativo utilizzato sul PC.

Software utilizzato: software applicativo utilizzato per il lavoro (es. SISSI, OFFICE, STAROFFICE, ecc...).

Rete: si indica se il PC è connesso alla rete.

Procedure di copia: indicazione di supporti e modalità per le copie di riserva.

MI SURE DI CARATTERE ELETTRONICO/INFORMATICO ADOTTATE PER GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI

Le misure di carattere elettronico/informatico² adottate sono:

- utilizzo di server con configurazioni di ridondanza protetto con firewall + antivirus + credenziali di autenticazione (Symantec Endpoint Protection) configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico e la scansione periodica dei supporti di memoria;
- presenza di gruppi di continuità per il server APC BACK UPS RS 800;
- impostazione e riconfigurazione di rete mediante HUB 8 porte;
- server collegato alla rete esterna tramite centralino sito nell'edificio comunale di Felizzano;
- attivazione di un sistema di backup centralizzato e automatizzato con periodicità giornaliera mediante HARD DISK ESTERNO PACKARD BELL 1,81 TB;
- installazione di firewall + antivirus + credenziali di autenticazione (Symantec Endpoint Protection) per ogni PC con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet;
- Live Update automatico e scansione del sistema periodica per ogni postazione protetta;
- Rinnovo abbonamento e aggiornamento annuale del sistema antivirus adottato;
- Definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi, Windows XP e Windows 7, di seguito specificate;
- definizione delle regole per la gestione di strumenti elettronico/informatico, di seguito specificate;
- definizione delle regole di comportamento per minimizzare i rischi di virus, di seguito riportate;
- separazione della rete locale delle segreterie da quella dei laboratori.

REGOLE PER LA GESTIONE DELLE PASSWORD³

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale e password personale.

User-id e password iniziali sono assegnati dal custode delle password.

User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.

L'user-id è costituita da 8 caratteri che corrispondono alle prime otto lettere del cognome ed eventualmente del nome. In caso di omonimia si procede con le

¹ Supporto procedura di backup: IOMEGA REV 35GB, giornaliero, alternando il supporto (giorni pari / giorni dispari)

² Le misure di carattere elettronico/informatico sono quelle in grado di segnalare gli accessi agli elaboratori, agli applicativi, ai dati e alla rete, di gestire le copie di salvataggio dei dati e degli applicativi, di assicurare l'integrità dei dati, di proteggere gli elaboratori da programmi volutamente o involontariamente ritenuti dannosi.

³ La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati: un corretto utilizzo della password è a garanzia dell'utente.

successive lettere del nome.

La password è composta da 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.

Ogni tre mesi ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.

Le password verranno automaticamente disattivate dopo sei mesi di non utilizzo.

Le password sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.

In caso di manutenzione straordinaria le credenziali di autenticazione di servizio possono essere comunicate, qualora necessario, dall'amministratore di sistema interno al tecnico/sistemista esterno addetto alla manutenzione. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.

Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:

- o la password deve essere costituita da una sequenza di massimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
- o al primo accesso la password ottenuta dal custode delle password deve essere cambiata;
- o la password deve essere cambiata ogni 3 mesi;
- o la password è segreta e non deve essere comunicata ad altri;
- o la password va custodita con diligenza e riservatezza;
- o l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia.

REGOLE PER LA GESTIONE DI STRUMENTI ELETTRONICO/INFORMATICO

Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:

- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
- le copie di backup realizzate su zip o su altro supporto, sono conservate nell'armadio di sicurezza, chiuso a chiave, poste nell'ufficio del D.S.G.A.
- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso.
- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
- divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.

La stampa di documenti contenenti dati sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

I fax si trovano in locali ad accesso controllato e il loro utilizzo è consentito unicamente agli incaricati del trattamento.

La manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il documento programmatico sulla sicurezza e di aver adottato le misure minime di sicurezza previste dal disciplinare.

REGOLE DI COMPORTAMENTO PER MINIMIZZARE I RISCHI DA VIRUS⁴

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC, XLS;
- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal responsabile del trattamento;
- disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);
- attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta, (in quanto potrebbe essere falso e portare a un sito-truffa);
- non utilizzare le chat;
- non attivare le condivisioni dell'HD in scrittura.
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

⁴ Le più recenti statistiche internazionali citano il virus informatico come la minaccia più ricorrente ed efficace

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

1. formattare l'Hard Disk;
2. definire le partizioni e reinstallare il Sistema Operativo. (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
3. installare il software antivirus, verificare e installare immediatamente gli eventuali ultimi aggiornamenti;
4. reinstallare i programmi applicativi a partire dai supporti originali;
5. effettuare il RESTORE dei soli dati a partire da una copia di backup recente. **NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;**
6. effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
7. ricordare all'utente di prestare particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.
8. provvedere ad aggiornare i dati del sistema nel più breve tempo possibile.

INCIDENT RESPONSE E RIPRISTINO⁵

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli user-id;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone si procede a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. spegnere correttamente il sistema oggetto dell'incidente
4. Una volta spento il sistema oggetto dell'incidente non deve più essere riaccessibile⁶;
5. documentare tutte le operazioni.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'amministratore di sistema, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide.

Altrimenti il titolare del trattamento, il responsabile del trattamento e l'amministratore di sistema coinvolgeranno esperti e/o autorità competenti. La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di incident

⁵ Un incidente può essere definito come un evento che produce effetti negativi sulle operazioni del sistema e che si configura come frode, danno, abuso, compromissione dell'informazione, perdita di beni.

⁶ E' indispensabile che per una eventuale indagine venga assicurata l'integrità e la sicurezza dello stato del sistema in oggetto e quindi non venga introdotta alcuna alterazione ai dati residenti nel sistema medesimo; un ripristino affrettato del sistema potrebbe alterare le prove dell'incidente.

response, tenendo presente quanto sotto indicato:

1. eseguire una copia bit to bit degli hard disk del sistema compromesso;
2. se l'incidente riguarda i dati il restore dei dati può avvenire sulla copia di cui al punto 1 precedente a partire dalle ultime copie di backup ritenute valide;
3. se l'incidente riguarda il sistema operativo o esiste la possibilità che sia stato installato software di tipo MMC il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto.

Tabella 3 - Procedure di spegnimento

Sistema operativo	Azione
Windows XP	<ol style="list-style-type: none">1. Fotografare lo schermo e documentare i programmi che sono attivi.2. Staccare la spina dalla presa di corrente.
Windows 7	<ol style="list-style-type: none">1. Fotografare lo schermo e documentare i programmi che sono attivi.2. Staccare la spina dalla presa di corrente.

Documento programmatico sulla sicurezza (ai sensi del D.L.vo n.196 del
30/06/2003)

ALLEGATO 4 – Regolamento per l'utilizzo della rete.

Articolo 1
OGGETTO E AMBITO DI APPLICAZIONE

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica dell'ISTITUTO in particolare per gli uffici di segreteria e di direzione, e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

La rete dell'ISTITUTO è connessa alla rete Internet.

Articolo 2
PRINCIPI GENERALI – DIRITTI E RESPONSABILITÀ

L'ISTITUTO promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità.

Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.

Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.

Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.

Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema. L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.

Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.

Articolo 3
ABUSI E ATTIVITÀ VIETATE

E' vietato ogni tipo di abuso¹. In particolare è vietato:

- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale dell'ISTITUTO;
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne a quella dell'ISTITUTO;
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;

¹ Si intende con abuso qualsiasi violazione del presente regolamento e di altre norme civili, penali e amministrative che disciplinano le attività e i servizi svolti sulla rete e di condotta personale.

- agire deliberatamente con attività che distruggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);
- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;
- cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- rimuovere, danneggiare deliberatamente o asportare componenti hardware.
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica dell'ISTITUTO per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere, copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
- inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;
- abbandonare il posto di lavoro lasciandolo incustodito o accessibile, come specificato nell'allegato 3.

Articolo 4 ATTIVITÀ CONSENTITE

E' consentito all'amministratore di sistema:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password come da procedura descritta nell'allegato 3;
- rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno

rispetto di quanto previsto riguardo ai diritti dei lavoratori.

Articolo 5 SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE

Hanno diritto ad accedere alla rete dell'ISTITUTO tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.

L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature. L'amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.

Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili l'amministratore di sistema può proporre al titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.

L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

Articolo 6 MODALITÀ DI ACCESSO ALLA RETE E AGLI APPLICATIVI

Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente.

L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete e si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.

L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.

L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus.

Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave) comunicatagli dal custode delle password e rispettare le norme indicate nell'allegato 3.

Articolo 7 SANZIONI

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti dell'ISTITUTO.

L'utilizzo del proxy riguarda le misure procedurali relative all'identificazione e all'autenticazione degli utenti, le regole di utilizzo delle risorse hardware e software, le norme comportamentali e le responsabilità di ciascuno. Rientrano in questo aspetto le norme di comportamento interno per limitare l'uso privato di e-mail o Internet, in quanto i controlli sono possibili solo a determinate condizioni e con l'accordo delle rappresentanze sindacali unitarie. Si ricorda che il D.L.vo 196/03 (Codice in materia di protezione dei dati personali) ribadisce quanto dettato dall'art. 4 dello Statuto dei Lavoratori, ovvero il "... divieto di utilizzo da parte del datore di lavoro di apparecchiature atte al controllo a distanza dell'attività del lavoratore, salvo che esigenze organizzative, produttive o di sicurezza non abbiano determinato, previo accordo con le rappresentanze sindacali, la lecita introduzione in azienda". D'altro canto la consultazione di siti web da parte del lavoratore o l'utilizzo di posta elettronica durante il normale orario di lavoro non è consentita quando tale attività non sia pertinente con le mansioni affidate, come l'art. 1024 del codice civile prevede nel principio generale di diligenza del lavoratore. Per trovare un punto di equilibrio tra i diritti del lavoratore e dell'istituto è opportuno introdurre una policy trasparente e codificata con l'apporto dei lavoratori, dando anche la possibilità al datore di lavoro di prevedere meccanismi sanzionatori, sempre che la policy sia resa accessibile a tutti i lavoratori, come previsto dall'art. 7 dello Statuto dei Lavoratori. Sempre tra le politiche di sicurezza si può fare riferimento alle responsabilità civili e penali per i danni cagionati con il trattamento dei dati personali. A titolo di esempio si possono elencare:

1. la responsabilità civile disciplinata dall'art. 2050 del Codice Civile e art. 15 D.Lgs. 196/03 "chi cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto a risarcire il danno, a meno che non provi di aver adottato tutte le misure idonee per evitarlo";
2. la sanzione penale che colpisce chi, essendovi tenuto, omette di adottare le misure di sicurezza (art. 169 del D.Lgs. 196/03), pari all'arresto fino a due anni o ad ammenda da 10mila a 50mila euro, ma con estinzione del reato in caso di regolarizzazione entro 6 mesi dall'accertamento del reato e pagamento di somma determinata dal Garante.

Le informazioni e le attività eseguite sulla rete informatica e telematica dell'Istituto Comprensivo "G. Pascoli" di Felizzano – P.zza P.Ercole 6 15023 Felizzano (AL) relative agli utilizzatori, sono registrate e conservate su file (registro elettronico delle attività o file di log).

Tali file possono essere soggetti ad indagini, nel rispetto di quanto sancito dal D.L.vo 30 giugno 2003, n. 196. Inoltre, il responsabile per la sicurezza può accedere ai file degli utilizzatori per proteggere l'integrità dei sistemi informatici. Per il regolamento d'uso della rete (policy) vedere l'Allegato 4.

Prot. n. 930/B19-C27-D17

Felizzano, 31.03.2015

INFORMATIVA EX ART. 13 D.LVO. N. 196/2003 PER IL TRATTAMENTO DEI DATI PERSONALI
DEGLI ALUNNI E DELLE LORO FAMIGLIE
PER L’INTERA PERMANENZA NELLA NOSTRA ISTITUZIONE

Gentile Signore/Signora,

si informa che il D.Lvo. n. 196 del 30 giugno 2003 ("Codice in materia di protezione dei dati personali") prevede la tutela delle persone fisiche e giuridiche rispetto al trattamento dei dati personali.

Secondo la normativa indicata, il trattamento dei dati personali da Lei comunicati, sarà effettuato da questa scuola secondo i principi di correttezza, liceità, trasparenza e di tutela della riservatezza e dei diritti degli alunni e delle rispettive famiglie.

I soggetti che trattano i dati nell’ambito dell’istituzione scolastica sono:

- a) il Dirigente Scolastico, il Direttore dei Servizi Generali Amministrativi, gli incaricati del trattamento amministrativo, il collaboratore vicario, tutti vincolati all’assoluta riservatezza;
- b) i docenti strettamente interessati (esclusivamente per i dati necessari alle attività didattiche, di valutazione, integrative e istituzionali);
- c) i collaboratori scolastici e i componenti gli Organi Collegiali (Consiglio di Istituto, Collegio Docenti, consigli di intersezione, di interclasse, di classe) limitatamente ai dati strettamente necessari alle loro attività.

I dati personali potranno essere comunicati ad altri enti pubblici e privati soltanto nei casi previsti da leggi e regolamenti. I dati personali potranno inoltre essere comunicati, insieme ai necessari documenti originali, ad altra scuola al fine di consentire il trasferimento nelle modalità previste dalle norme sull’ Istruzione Pubblica.

Ai sensi dell'articolo 13 del D.lvo. n.196/2003, pertanto, La informiamo che:

1. titolare del trattamento è la scuola stessa, che ha personalità giuridica autonoma ed è legalmente rappresentata dal Dirigente Scolastico in carica, elettivamente domiciliato presso la scuola;
2. responsabile del trattamento dei dati relativi ad alunni, dipendenti, collaboratori esterni e fornitori, affari generali e protocollo è il Direttore dei Servizi Generali Amministrativi, elettivamente domiciliato presso la Scuola;
3. i dati personali da Lei forniti verranno trattati esclusivamente per le finalità istituzionali della scuola, che sono quelle dell’ istruzione e formazione degli alunni nonché quelle amministrative ad esse strumentali.
4. I dati saranno trattati con modalità manuali e/o con l’ausilio di strumenti elettronici o comunque automatizzati, secondo le modalità e le cautele previste dal predetto D.L.vo. Saranno conservati per il tempo necessario all’espletamento delle attività amministrative e istituzionali riferibili alle predette finalità oltre che negli archivi presenti presso l’Istituto, anche presso archivi del Ministero dell’Istruzione (MIUR) e/o in altri database gestiti da soggetti pubblici (Ufficio Scolastico Regionale, Ufficio Scolastico Territoriale, Amministrazione Provinciale, ...);
5. Il conferimento dei dati che Le vengono richiesti è obbligatorio per consentire alla scuola di adempiere a tutte le formalità scolastiche che altrimenti non potrebbero aver luogo, precludendo così la possibilità di fornire all’alunno tutti i servizi necessari per garantire il suo diritto all’istruzione e alla formazione.
6. I dati personali “sensibili” o “giudiziari” raccolti non saranno oggetto di diffusione; potranno tuttavia essere comunicati ad altri soggetti pubblici se ed in quanto ciò si renda necessario per lo svolgimento delle attività istituzionali previste dalle vigenti disposizioni in materia sanitaria o giudiziaria. *Si ricorda che i dati definiti “sensibili” sono quelli “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 o la vita sessuale”. I dati “giudiziari” sono invece quelli “idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale”.*
7. I dati raccolti, trattati ciascuno limitatamente ai propri ambiti di competenza dai docenti e dal personale di segreteria dipendente dall’Istituto, possono essere comunicati in particolare a: società di assicurazione per infortuni e responsabilità civile, aziende esterne incaricate di fornire servizi alla scuola, Enti Locali per fini istituzionali, Enti di Formazione Professionale per attività di orientamento, aziende di trasporto pubblico e privato preposte per il servizio di trasporto alunni, autorità di polizia e giudiziarie per indagini ed accertamenti;

8. i soli dati identificativi degli alunni possono venire pubblicati sul sito web dell'Istituto per facilitare la comunicazione con le famiglie, soprattutto in merito alla formazione delle classi;
9. con le finalità di documentazione, è possibile che fotografie che ritraggono gli alunni nello svolgimento delle attività scolastiche curriculari, integrative o complementari, vengano pubblicate sul sito web dell'Istituto e/o quello di portali scolastici dedicati, quali Resmo, Indire, Bdp Ad inizio dell'Anno Scolastico viene richiesta ai genitori la sottoscrizione di una liberatoria. In ogni momento la famiglia potrà richiedere (compilando l'apposito modulo disponibile in segreteria) l'immediata cancellazione o l'oscuramento delle foto che riguardano l'alunno eventualmente pubblicate su detti siti;
10. al Titolare del trattamento o al Responsabile, Lei potrà rivolgersi senza particolari formalità per far valere i Suoi diritti, così come previsto dall'articolo 7 del D.L.vo 196/2003, qui di seguito riportato:

**Art. 7 del Decreto Legislativo n.196/2003
(Diritto di accesso ai dati personali ed altri diritti)**

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intellegibile.
2. L'interessato ha diritto di ottenere l'indicazione:
 - a) dell'origine dei dati personali;
 - b) delle finalità e modalità del trattamento;
 - c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
 - d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
 - e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o dei quali possono venire a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
 - a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
 - b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
 - c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
 - a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
 - b) al trattamento di dati personali che lo riguardano ai fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Copia della presente informativa, già pubblicata all'Albo dell'Istituto, viene consegnata alla famiglia dell'alunno. Copia firmata per ricevuta e presa visione è conservata dalla segreteria.
Il trattamento dei dati per le finalità di legge verrà comunque effettuato.

IL DIRIGENTE SCOLASTICO
Dott.ssa Maria Paola MINETTI

Il/La sottoscritto/a	cognome e nome del genitore
genitore di (responsabile dell'obbligo)	cognome e nome dell' alunno/a
frequentante la scuola	indicare il tipo di scuola e la sede della scuola
dichiara di aver ricevuto l'informativa (e di averne presa visione) di cui all'art. del D.L.vo 196/2003.	
Per presa visione (firma obbligatoria)	Per accettazione

ISTITUTO COMPRENSIVO “G. PASCOLI”
di Scuola dell’Infanzia, Primaria e Secondaria di I Grado
P.zza Paolo Ercole, 6 – 15023 Felizzano (AL)
Tel.0131-791122 – FAX 0131-791395 - CF96034370062
www.icpascoli-felizzano.gov.it - email: icpascoli-felizzano@libero.it

Prot. n. 930/A2

Felizzano, 31.03.2015

INFORMATIVA EX ART. 13 D.LVO. N. 196/2003 PER IL TRATTAMENTO DEI DATI PERSONALI
DEL PERSONALE DIPENDENTE PER L'INTERA PERMANENZA NELLA NOSTRA ISTITUZIONE

Al Personale dipendente/collaboratore

Gentile Signore/Signora,

si informa che il D.Lvo. n. 196 del 30 giugno 2003 ("Codice in materia di protezione dei dati personali") prevede la tutela delle persone fisiche e giuridiche rispetto al trattamento dei dati personali.

Secondo la normativa indicata, il trattamento dei dati personali che La riguardano, da Lei comunicati o altrimenti acquisiti e quelli eventuali dei Suoi familiari, sarà effettuato da questa scuola secondo i principi di correttezza, liceità, trasparenza e di tutela della riservatezza e dei diritti del personale dipendente/collaboratore.

I soggetti che trattano i dati nell’ambito dell’istituzione scolastica sono:

- a) il Dirigente Scolastico, il Direttore dei Servizi Generali Amministrativi, gli incaricati del trattamento amministrativo, il collaboratore vicario, tutti vincolati all’assoluta riservatezza;
- b) i docenti strettamente interessati (esclusivamente per i dati necessari alle attività didattiche, di valutazione, integrative e istituzionali);
- c) i collaboratori scolastici e i componenti gli Organi Collegiali (Consiglio di Istituto, Collegio Docenti, consigli di intersezione, di interclasse, di classe) limitatamente ai dati strettamente necessari alle loro attività.

I dati personali potranno essere comunicati ad altri enti pubblici e privati soltanto nei casi previsti da leggi e regolamenti. I dati personali potranno inoltre essere comunicati, insieme ai necessari documenti originali, ad altra scuola al fine di consentire il trasferimento, nelle modalità previste dalle norme sull’ Istruzione Pubblica.

Ai sensi dell'articolo 13 del D.lvo. n.196/2003, pertanto, La informiamo che:

1. titolare del trattamento è la scuola stessa, che ha personalità giuridica autonoma ed è legalmente rappresentata dal Dirigente Scolastico in carica, elettivamente domiciliato presso la scuola;
2. responsabile del trattamento dei dati relativi ad alunni, dipendenti, collaboratori esterni e fornitori, affari generali e protocollo è il Direttore dei Servizi Generali Amministrativi, elettivamente domiciliato presso la Scuola;
3. i dati personali da Lei forniti verranno trattati esclusivamente per le finalità istituzionali della scuola, in particolare per le finalità della gestione del Suo rapporto di lavoro/collaborazione in tutti i suoi aspetti contrattuali, previdenziali, assicurativi, fiscali e per gli altri compiti che la Legge affida al datore di lavoro/committente;
4. i dati saranno trattati con modalità manuali e/o con l’ausilio di strumenti elettronici o comunque automatizzati, secondo le modalità e le cautele previste dal predetto D.L.vo. Saranno conservati per il tempo necessario all’espletamento delle attività amministrative e istituzionali riferibili alle predette finalità, oltre che negli archivi presenti presso l’Istituto, anche presso archivi del Ministero dell’Istruzione (MIUR) e/o in altri database gestiti da soggetti pubblici (Ufficio Scolastico Regionale, Ufficio Scolastico Territoriale, Amministrazione Provinciale, ...);
5. il conferimento dei dati che Le vengono richiesti è obbligatorio in quanto necessario per gli adempimenti connessi e conseguenti al rapporto di lavoro. L’eventuale rifiuto di fornire tali dati comporta il mancato perfezionamento o mantenimento del rapporto di lavoro stesso;
6. gli eventuali dati personali “sensibili” o “giudiziari”, da Lei forniti alla scuola, non saranno oggetto di diffusione; potranno tuttavia essere comunicati ad altri soggetti pubblici se ed in quanto ciò si renda necessario per lo svolgimento delle attività istituzionali previste dalle vigenti disposizioni in materia sanitaria o giudiziaria e per la gestione del rapporto di lavoro. *Si ricorda che i dati definiti “sensibili” sono quelli “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 o la vita sessuale”. I dati “giudiziari” sono invece quelli “idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale”..*

7. I dati personali raccolti, trattati ciascuno limitatamente ai propri ambiti di competenza dal personale di segreteria dell'Istituto, possono essere comunicati e trasferiti sul territorio nazionale alle seguenti categorie di soggetti: Enti Pubblici (MIUR, Ufficio Scolastico Regionale, ex Centro Servizi Amministrativi – Ufficio Scolastico Territoriale - , Amministrazione Provinciale, ...) INPS, INPDAP, INAIL, Centro per l'impiego, Direzione Provinciale dei Servizi Vari, Ragioneria Provinciale dello Stato , Ministero delle Finanze, ASL , autorità di polizia, società di assicurazione, Fondi o Casse (anche private) di previdenza e assistenza, ditte esterne incaricate di adempimenti connessi al rapporto di lavoro, CAF, organizzazioni sindacali ed altri soggetti sempre e solo connessi al Suo rapporto di lavoro dietro Sua esplicita richiesta per la fruizione di servizi aggiuntivi;
8. i soli dati identificativi possono essere pubblicati sul sito web dell'Istituto per motivi organizzativi e per facilitare la comunicazione interna e con le famiglie (ad esempio, per i docenti: composizione dei consigli di classe e orari di ricevimento settimanale, orario delle lezioni,.....);
9. con le finalità di documentazione, è possibile che fotografie che ritraggono alunni, docenti e personale nello svolgimento delle attività curriculari, integrative o complementari siano state pubblicate sul sito web dell'Istituto e/o quello di portali scolastici dedicati, quali Resmo, Indire, Bdp In ogni momento l'interessato potrà chiedere (compilando l'apposito modulo disponibile in segreteria) l'immediata cancellazione o l'oscuramento delle foto che lo riguardano eventualmente pubblicate su detti siti;
10. al Titolare del trattamento o al Responsabile, Lei potrà rivolgersi senza particolari formalità per far valere i Suoi diritti, così come previsto dall'articolo 7 del D.L.vo 196/2003, qui di seguito riportato:

**Art. 7 del Decreto Legislativo n.196/2003
(Diritto di accesso ai dati personali ed altri diritti)**

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intellegibile.
2. L'interessato ha diritto di ottenere l'indicazione:
 - a) dell'origine dei dati personali;
 - b) delle finalità e modalità del trattamento;
 - c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
 - d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
 - e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o dei quali possono venire a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
 - a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
 - b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
 - c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
 - a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
 - b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Copia della presente informativa, già pubblicata all'Albo dell'Istituto, è consegnata al dipendente/collaboratore. Copia firmata per ricevuta e presa visione è conservata dalla segreteria.

Il trattamento dei dati per le finalità di legge verrà comunque effettuato.

Il Dirigente Scolastico
Dott.ssa Maria Paola MINETTI

Il/La sottoscritto/a	cognome e nome del dipendente
nella sua qualità di	qualifica all'interno dell'Istituzione Scolastica
dichiara di aver ricevuto l'informativa di cui all'art. 13 del D.L.vo 196/2003.	
Per presa visione	Per accettazione
firma leggibile	firma leggibile



ISTITUTO COMPRESIVO "G. PASCOLI"
di Scuola dell'Infanzia, Primaria e Secondaria di I Grado
Piazza Paolo Ercole, 6 – 15023 Felizzano (AL)
Tel.0131/791122 – FAX 0131/791395 – C.F. 96034370062
www.icpascoli-felizzano.gov.it - email: icpascoli-felizzano@libero.it

Al sig. _____

Oggetto: Legge 196/2003 "Codice in materia di protezione dei dati personali". Informativa all'interessato.

Secondo quanto previsto dall'art. 13 del D. LGS 196/2003 "Codice in materia di protezione dei dati personali" recante disposizioni sulla tutela della persona e di altri soggetti rispetto al trattamento di dati personali, questa Istituzione Scolastica, rappresentata dal dirigente scolastico **Dott.ssa Maria Paola MINETTI** in qualità di Titolare del trattamento dei dati personali, per espletare le sue funzioni istituzionali e in particolare per gestire i rapporti contrattuali instaurati in data deve acquisire o già detiene dati personali che La riguardano.

La informiamo inoltre che il trattamento dei suoi dati personali avrà le seguenti finalità:

- elaborazione, liquidazione e corresponsione degli importi dovuti e relativa contabilizzazione;
- adempimento di obblighi derivanti da leggi, contratti, regolamenti in materia di igiene e sicurezza del lavoro, in materia fiscale, in materia assicurativa;
- tutela dei diritti in sede giudiziaria.

Le forniamo a tal fine le seguenti ulteriori informazioni:

- Il trattamento dei Suoi dati personali sarà improntato a principi di correttezza, liceità e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti.
- I Suoi dati personali verranno trattati anche con l'ausilio di strumenti elettronici o comunque automatizzati con le modalità e le cautele previste dal predetto D. LGS e conservati per il tempo necessario all'espletamento delle attività istituzionali e amministrative riferibili alle predette finalità
- Il titolare del trattamento è il dirigente scolastico dott.ssa Maria Paola Minetti.
- Il responsabile del trattamento è il Direttore dei Servizi Generali e Amministrativi Maria Teresa Messoriano.
- L'incaricata al trattamento è l'assistente amministrativo Anna Viotti espressamente autorizzata all'assolvimento di tali compiti, identificati ai sensi di legge, ed edotta dei vincoli imposti dal D.Lgs. n. 196/2003;
- I dati oggetto di trattamento potranno essere comunicati ai seguenti soggetti esterni all'istituzione scolastica per fini funzionali:
MIUR, Ufficio Scolastico Territoriale, Revisori dei Conti.

Le ricordiamo infine:

- che il conferimento dei dati richiesti è indispensabile a questa istituzione scolastica per l'assolvimento dei suoi obblighi istituzionali, pertanto il mancato consenso al trattamento può comportare il mancato o parziale espletamento di tali obblighi;
- che in ogni momento potrà esercitare i Suoi diritti nei confronti del titolare del trattamento, ai sensi dell'art. 7 del D. LGS 196/2003 riportato in calce alla presente comunicazione.

II DIRIGENTE SCOLASTICO
Dott.ssa Maria Paola MINETTI

Il sottoscritto _____

acquisita, attentamente letta e compresa, la presente informativa fornita dal titolare del trattamento ai sensi dell'art. 13 del D.Lgs. 196/2003, compresi gli articoli citati del D.Lgs. 196/2003

- acconsente al trattamento dei propri dati personali.

Data

firma

ALLEGATO ALL'INFORMATIVA

Decreto Legislativo n. 196/2003.

Art. 7 - Diritto di accesso ai dati personali ed altri diritti

1- L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati e la loro comunicazione in forma intelligibile.

2- L'interessato ha diritto di ottenere l'indicazione:

- a) dell'origine dei dati personali;
- b) delle finalità e modalità del trattamento;
- c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5, comma 2;
- e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello stato, di responsabili o incaricati .

3- L'interessato ha diritto di ottenere:

- a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse , l'integrazione dei dati;
- b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4- L'interessato ha diritto ad opporsi, in tutto o in parte:

- a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.



ISTITUTO COMPRENSIVO "G. PASCOLI"
di Scuola dell'Infanzia, Primaria e Secondaria di I Grado
Piazza Paolo Ercole, 6 – 15023 Felizzano (AL)
Tel.0131/791122 – FAX 0131/791395 – C.F. 96034370062

www.icpascoli-felizzano.gov.it - email: icpascoli-felizzano@libero.it

Prot. n. 930/A2

Felizzano, 31.03.2015

INFORMATIVA SITOWEB

L'Istituto Comprensivo "G.Pascoli" di Felizzano rispetta la privacy dei propri utenti e si impegna a proteggere i loro dati personali.

In generale, l'utente può navigare sul sito web dell'Istituto Comprensivo all'indirizzo: www.icpascoli-felizzano.gov.it senza fornire alcun tipo di informazione personale. La raccolta ed il trattamento di dati personali avvengono quando necessari in relazione all'esecuzione di servizi richiesti dall'utente, o quando l'utente stesso decide di comunicare i propri dati personali; in tali circostanze, il presente regolamento della privacy illustra le modalità ed i caratteri di raccolta e trattamento dei dati personali dell'utente. L'Istituto Comprensivo "G.Pascoli" di Felizzano tratta i dati personali forniti dagli utenti in conformità alla normativa vigente.

Raccolta di Dati Personali

Dato personale significa qualsiasi informazione che possa essere impiegata per identificare un individuo, una società od altro ente. A titolo puramente esemplificativo e non esaustivo viene raccolto ad esempio il nome ed il cognome, l'indirizzo di posta elettronica (e-mail), l'indirizzo, un recapito postale od altro recapito di carattere fisico, altre informazioni necessarie per contattare l'utente, qualifica, data di nascita, genere, lavoro, attività commerciale, interessi personali, altre informazioni necessarie per la prestazione di servizi richiesti dall'utente.

La navigazione sul sito dell'Istituto Comprensivo "G.Pascoli" di Felizzano avviene in forma anonima, a meno che l'utente abbia precedentemente specificato che desidera che l'Istituto Comprensivo "G.Pascoli" di Felizzano ricordi l'identificativo con cui si è registrato e la relativa password. L'Istituto Comprensivo "G.Pascoli" di Felizzano non compie operazioni di raccolta dati dell'utente con modalità automatiche, incluso l'indirizzo di posta elettronica (e-mail). L'Istituto Comprensivo "G.Pascoli" di Felizzano registra l'indirizzo IP dell'utente (Internet Protocol, vale a dire l'indirizzo Internet del computer dell'utente) per avere un'idea dell'area del sito che l'utente visita e della durata della visita, nel rispetto della normativa vigente in tema di tutela di dati personali. Tuttavia l'Istituto Comprensivo "G.Pascoli" di Felizzano non mette in relazione l'indirizzo IP dell'utente con altre informazioni personali relative allo stesso, se non dopo averlo debitamente informato del relativo trattamento ed avere ottenuto il suo consenso al trattamento, e solo rispetto ad utenti registrati al sito dell' istituto (nome dell'istituzione scolastica) Come molti altri siti web aventi carattere e contenuto indirizzato ai servizi, il sito dell'Istituto Comprensivo "G.Pascoli" di Felizzano può impiegare una tecnologia standard chiamata "cookie" per raccogliere informazioni sulle modalità di uso del sito da parte dell'utente. Per ulteriori informazioni, l'utente è invitato a consultare la seguente sezione "Cookies".

L'Istituto Comprensivo "G.Pascoli" di Felizzano raccoglie i dati personali dell'utente in occasione della sua registrazione, per emettere un account, necessario all'utente per usufruire di determinati prodotti o servizi.

In particolare la registrazione è necessaria all'utente per partecipare al forum, per usufruire della chat, per poter inviare messaggi ad altri iscritti, per inserire commenti alle notizie, quando l'utente chiede di ricevere determinate e-mail o di essere inserito in una mailing list, o quando l'utente, per qualsiasi altra ragione, comunica i propri dati personali.

L'Istituto Comprensivo "G.Pascoli" di Felizzano usa tali informazioni solamente ove le stesse siano state legittimamente raccolte, in conformità al presente Regolamento della Privacy e nel rispetto della normativa vigente.

Comunicazione di Dati Personali

In caso di raccolta di dati personali, l'Istituto Comprensivo "G.Pascoli" di Felizzano informerà l'utente delle finalità della raccolta al momento della stessa e, ove necessario, richiederà il consenso dell'utente. L'Istituto Comprensivo "G.Pascoli" di Felizzano non comunicherà i dati personali dell'utente a terzi senza il consenso dell'utente, salvo le limitate circostanze specificate in seguito nella Sezione "Ambito di Comunicazione e Diffusione di Dati Personali".

Se l'utente decide di fornire all'Istituto Comprensivo "G.Pascoli" di Felizzano i propri dati personali, l'Istituto Comprensivo "G.Pascoli" di Felizzano potrà comunicarli all'interno dell'Istituto o a terzi che prestano servizi all'istituto, che hanno bisogno di conoscerli in ragione delle proprie mansioni, e, ove necessario, con il permesso dell'utente. L'Istituto Comprensivo "G.Pascoli" di Felizzano invierà all'utente materiale relativo ad attività di informazione ed a ricerche di mercato solo dopo aver informato l'utente ed aver ottenuto il consenso dello stesso al trattamento, in conformità alle disposizioni vigenti in tema di protezione di dati personali.

Cookies

Un cookie è un piccolo file di testo che alcuni siti web inviano all'hard drive dell'utente in occasione della visita al sito. Un cookie può contenere informazioni quali un ID dell'utente che il sito usa per controllare le pagine visitate, ma le uniche informazioni di carattere personale che un cookie può contenere sono quelle fornite dall'utente stesso. Un cookie non può leggere i dati presenti sull'hard disk dell'utente o leggere i cookies creati da altri siti. Alcune aree del sito web dell'Istituto Comprensivo "G.Pascoli" di Felizzano impiegano cookies per registrare le modalità di navigazione degli utenti sul sito. L'Istituto Comprensivo "G.Pascoli" di Felizzano si serve di cookies per determinare il grado di utilità delle informazioni che fornisce ai propri utenti e per verificare l'efficacia della struttura di navigazione del sito, in relazione al supporto aiuto offerto all'utente per ottenere quell'informazione.

Se l'utente non desidera ricevere cookies durante la navigazione sul sito, può programmare il proprio browser in modo da essere avvertito prima di accettare cookies e rifiutare i cookies quando il browser avvisa della presenza di cookies. L'utente può anche rifiutare tutti i cookies, disattivandoli nel proprio browser, anche se in tal modo l'utente non sarebbe poi in grado di beneficiare in pieno dei vantaggi del sito dell'Istituto Comprensivo "G.Pascoli" di Felizzano. In particolare, all'utente potrebbe essere chiesto di accettare cookies al fine di compiere determinate operazioni sul sito web dell'Istituto Comprensivo "G.Pascoli" di Felizzano. Tuttavia non è necessario che l'utente accetti tutti i cookies per usare /navigare in molte aree del sito, salvo il caso in cui per l'accesso a specifiche pagine web dell'Istituto Comprensivo "G.Pascoli" di Felizzano siano necessari la registrazione ed una password.

Finalità e Modalità di Trattamento dei Dati Raccolti

L'Istituto Comprensivo "G.Pascoli" di Felizzano tratta i dati personali dell'utente per le seguenti finalità di carattere generale: per soddisfare le richieste relative a specifici prodotti o servizi, per personalizzare la visita dell'utente al sito, per aggiornare l'utente sulle ultime novità in relazione ai propri servizi, od altre informazioni che l'istituto ritiene siano di interesse dell'utente, e che provengono dall'Istituto Comprensivo "G.Pascoli" di Felizzano o dai suoi partners, e per comprendere meglio i bisogni dell'utente ed offrire allo stesso servizi migliori. Il trattamento di dati personali dell'utente da parte dell'Istituto Comprensivo "G.Pascoli" di Felizzano per le finalità sopra specificate avviene in conformità alla normativa vigente a tutela di dati personali.

Ambito di Comunicazione e Diffusione di Dati Personali

I dati personali dell'utente non vengono comunicati al di fuori della realtà dell'Istituto Comprensivo "G.Pascoli" di Felizzano senza il consenso dell'interessato, salvo quanto di seguito specificato.

Nell'ambito dell'organizzazione dell'Istituto Comprensivo "G.Pascoli" di Felizzano, i dati sono conservati in server controllati, cui è consentito un accesso limitato in conformità alla normativa vigente a tutela di dati personali.

L'Istituto Comprensivo "G.Pascoli" di Felizzano può comunicare i dati personali dell'utente a terzi in uno dei seguenti casi: quando l'interessato abbia prestato il proprio consenso alla comunicazione; quando la comunicazione sia necessaria per fornire il prodotto od il servizio richiesto dall'utente; quando la comunicazione sia necessaria in relazione a terzi che lavorano per conto dell'istituto per fornire il prodotto od il servizio richiesto dall'utente (Comprensivo

"G.Pascoli" di Felizzano comunicherà a questi solo le informazioni che si rendono necessarie in relazione alla prestazione del servizio, ed alle stesse è vietato trattare i dati per finalità diverse); o per fornire all'utente le informazioni che l'Istituto Comprensivo "G.Pascoli" di Felizzano ritenga sia interessato a conoscere dall'istituto stesso e dagli altri enti ad esso collegati (in qualsiasi momento l'utente potrà richiedere di non ricevere più tale tipo di informazioni). L'Istituto Comprensivo "G.Pascoli" di Felizzano inoltre divulgherà i dati personali dell'utente in caso ciò sia richiesto dalla legge.

Diritti dell'Utente; User Account

Se l'utente è registrato, può avere accesso ai propri dati personali accedendo alla pagina in cui sono contenuti dalla voce di menù "Il mio PROFILO". L'utente può chiedere la cancellazione dalla newsletter, può limitare la diffusione della propria email o in generale del proprio profilo agli altri iscritti. Può chiedere la cancellazione del proprio account o qualsiasi altro proprio dato personale inviando una e-mail al seguente indirizzo (webmaster@icpascoli-felizzano.gov.it).

Sicurezza dei Dati

Le informazioni dell'account dell'utente sono protette da una password per garantire la riservatezza e la sicurezza dell'utente. L'Istituto Comprensivo "G.Pascoli" di Felizzano adotta tutte le misure di sicurezza e le procedure fisiche, elettroniche, ed organizzative richieste dalla normativa vigente. In alcune aree del proprio sito web, l'Istituto Comprensivo "G.Pascoli" di Felizzano impiega sistemi standard SSL di criptazione per aumentare la sicurezza della trasmissione di dati. Anche se fa quanto ragionevolmente possibile per proteggere i dati personali dell'utente, l'Istituto Comprensivo "G.Pascoli" di Felizzano non può garantire la completa totale sicurezza dei dati trasmessi dagli utenti durante la comunicazione, quindi l'Istituto Comprensivo "G.Pascoli" di Felizzano raccomanda caldamente all'utente di adottare misure precauzionali per proteggere i propri dati personali quando naviga su Internet. Ad esempio, l'utente è invitato a cambiare spesso la propria password, usare una combinazione di lettere e numeri, ed assicurarsi di fare uso di un browser sicuro.

I Minori e la Privacy

Il sito web dell'Istituto Comprensivo "G.Pascoli" di Felizzano è pensato per un utilizzo anche da parte di minori di 18 anni, in quanto presenta contenuti puramente didattici e culturali. Quindi l'Istituto Comprensivo "G.Pascoli" di Felizzano non richiede, in fase di iscrizione, la maggiore età dell'utente.

Siti di Terzi

Il sito web dell'Istituto Comprensivo "G.Pascoli" di Felizzano contiene links ad altri siti. L'Istituto Comprensivo "G.Pascoli" di Felizzano non condivide i dati personali dell'utente con questi siti e non è responsabile delle pratiche degli stessi, in relazione alla tutela ed al trattamento di dati personali. L'Istituto Comprensivo "G.Pascoli" di Felizzano invita l'utente a prendere visione delle politiche della privacy di tali siti per conoscere le modalità di trattamento e raccolta dei propri dati personali da parte di tali siti web di terzi.

Modifiche al Regolamento della Privacy

L'Istituto Comprensivo "G.Pascoli" di Felizzano modificherà periodicamente il presente Regolamento. Qualora modifichi in termini sostanziali le modalità di trattamento dei dati personali dell'utente, renderà disponibile tale informazione pubblicando apposita comunicazione sul proprio sito.

Domande o Suggerimenti

In caso di domande o dubbi in relazione alla raccolta, all'uso al trattamento, od alla comunicazione o diffusione dei propri dati personali, l'utente può inviare una e-mail al seguente indirizzo di posta elettronica: (webmaster@icpascoli-felizzano.gov.it).

Il presente documento è stato redatto e revisionato il 31.03.2015

Il Titolare del trattamento
Dirigente Scolastico
Dott.ssa Maria Paola MINETTI



ISTITUTO COMPRENSIVO "G. PASCOLI"
di Scuola dell'Infanzia, Primaria e Secondaria di I Grado
Piazza Paolo Ercole, 6 – 15023 Felizzano (AL)
Tel.0131/791122 – FAX 0131/791395 – C.F. 96034370062

www.icpascoli-felizzano.gov.it - email: icpascoli-felizzano@libero.it

Prot. n. 930/A2

Felizzano, 31.03.2015

All'Assistente Amministrativo
Sig.ra Migliardi Franca

Oggetto: Incarico di amministratore di sistema interno.

La sottoscritta Dott.ssa Maria Paola MINETTI non in proprio, ma in qualità di rappresentante legale dell'Istituto Comprensivo di Felizzano, titolare del trattamento dei dati ai sensi del D.L.vo n°196 del 30/06/2003, conformemente a quanto stabilito nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza", affida alla Sig.ra Migliardi Franca l'incarico di amministratore di sistema con i seguenti compiti:

1. Verificare che siano effettuate le copie di salvataggio;
2. accensione server di rete tramite password di sistema;
3. collaborare con il responsabile del trattamento dei dati personali;
4. collaborare con il custode delle password;
5. in caso di malfunzionamento interpellare la ditta incaricata e sovrintendere all'operato di eventuali tecnici esterni all'amministrazione.

L'amministratore testè incaricato dichiara di essere a conoscenza di quanto stabilito dal D.L.vo n°196 del 30/06/2003 ed in particolare di quanto indicato nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme descritte nel Documento Programmatico sulla Sicurezza, in relazione ai compiti sopra indicati.

Il Titolare del trattamento
DIRIGENTE SCOLASTICO
Dott.ssa Maria Paola MINETTI

Per accettazione dell'incarico
L'amministratore del sistema
(Franca Migliardi)



**ISTITUTO COMPRENSIVO “G. PASCOLI”
di Scuola dell’Infanzia, Primaria e Secondaria di I Grado**

Piazza Paolo Ercole, 6 – 15023 Felizzano (AL)

Tel.0131/791122 – FAX 0131/791395 – C.F. 96034370062

www.icpascoli-felizzano.gov.it - email: icpascoli-felizzano@libero.it

Prot. n. 930/A2

Felizzano, 31.03.2015

All’Assistente Amministrativo

Sig. Palla Riccardo

Oggetto: Incarico custode delle password

Conformemente a quanto previsto dal punto 10 del Disciplinare tecnico, allegato B) al D.Lgs. n.196/2003, in base al quale, quando vi sono più incaricati del trattamento e sono pertanto in uso più parole chiave, è necessario individuare per iscritto, i soggetti incaricati della custodia delle password, con la presente la nominiamo “incaricato della custodia delle password” necessarie per accedere agli elaboratori elettronici in uso presso gli uffici dell’Istituto Comprensivo “G.Pascoli” di Felizzano.

La S.V. dovrà usare la massima riservatezza e discrezione nella gestione delle password e nella loro protezione, anche con riferimento agli obblighi che Le derivano dalla qualifica professionale. In particolare, nello svolgimento di tale compito Lei dovrà:

- ricevere dagli incaricati del trattamento di dati personali con elaboratori elettronici la busta chiusa sulla quale è indicata la user-id contenente la password da essi elaborata e che essi hanno provveduto sostituire autonomamente con la prevista periodicità ;
- custodire le password attribuite dagli incaricati del trattamento di dati personali con elaboratori elettronici;
- revocare tutte le password non utilizzate per un periodo superiore a 6 mesi;
- revocare tempestivamente tutte le password assegnate a soggetti che su comunicazione scritta del responsabile del trattamento non sono più autorizzati ad accedere ai dati;
- nel caso in cui il titolare del trattamento abbia la necessità indifferibile di accedere ad un elaboratore in caso di prolungata assenza o impedimento dell’incaricato che lo utilizza abitualmente (per malattia, ferie, etc.), consegnare al titolare stesso la busta contenente la password dell’elaboratore sul quale egli può intervenire unicamente per necessità di operatività e sicurezza del sistema informativo (ad es., effettuazione di interventi di riparazione, assistenza, aggiornamento antivirus, etc.);
- informare tempestivamente l’incaricato del quale, in sua assenza, è stata consegnata la password al titolare del trattamento, affinché questi provveda immediatamente alla sostituzione della parola chiave e la consegna al custode in una nuova busta chiusa.
- gestire le buste contenenti le password degli incaricati del trattamento e conservarle in un luogo sicuro e protetto.

Il custode delle password testè incaricato dichiara di essere a conoscenza di quanto stabilito dal D.L.vo n° 196 del 30/06/2003 ed in particolare da quanto indicato nell’allegato B “Disciplinare tecnico in materia di misure minime di sicurezza” e si impegna ad adottare tutte le misure necessarie all’attuazione delle norme in esso descritte, in relazione ai compiti sopra indicati.

Il Titolare del trattamento

DIRIGENTE SCOLASTICO

Dott.ssa Maria Paola MINETTI

Per accettazione dell’incarico

Il custode delle password

(Riccardo Palla)



ISTITUTO COMPRENSIVO “G. PASCOLI”
di Scuola dell’Infanzia, Primaria e Secondaria di I Grado
P.zza Paolo Ercole, 6 – 15023 Felizzano (AL) - CF96034370062
Tel.0131-791122 – FAX 0131-791395

sitoweb : www.icpascoli.felizzano.gov.it

email: icpascoli-felizzano@libero.it – alic81800q@istruzione.it – PEC: alic81800q@pec.istruzione.it

Prot. n. 930/A2

Felizzano, 31.03.2015

Oggetto: Incarico di amministratore di sistema.

La sottoscritta dott.ssa Maria Paola MINETTI, non in proprio ma in qualità di rappresentante legale dell’Istituto Comprensivo “G. Pascoli” di Felizzano, titolare del trattamento dei dati ai sensi del D.L.vo n. 196 del 30/06/03, conformemente a quanto stabilito nell’allegato B “Disciplinare tecnico in materia di misure minime di sicurezza” affida alla ditta Informatica Service s.r.l, Via Ghilini 10, Alessandria, l’incarico di amministratore di sistema con i seguenti compiti:

- Sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, filtri);
- Monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- Effettuare interventi di manutenzione hardware e software su sistemi operativi e applicativi;
- Fare in modo che sia prevista la disattivazione dei codici identificativi personali (user-id), in caso di perdita della qualità che consentiva all’incaricato l’accesso al personal computer, oppure nel caso di mancato utilizzo del codice per oltre sei mesi;
- Gestire le password di root o di amministratore di sistema.

L’amministratore testé incaricato dichiara di essere a conoscenza di quanto stabilito dal D.L.vo n°196 del 30/06/2003 ed in particolare di quanto indicato nell’allegato B “Disciplinare tecnico in materia di misure minime di sicurezza” e si impegna ad adottare tutte le misure necessarie all’attuazione delle norme descritte nel Documento Programmatico sulla Sicurezza, in relazione ai compiti sopra indicati.

Il titolare del trattamento
DIRIGENTE SCOLASTICO
Dott.ssa Maria Paola MINETTI

Per accettazione dell’incarico
L’amministratore del sistema
(Informatica Service)

(firma)

LETTERA DI INCARICO: UNITA' ORGANIZZATIVA "DOCENTI"

IL DIRIGENTE SCOLASTICO E IL DSGA

visto:

- l'art. 30 del D.L.vo 196/2003 "Codice in materia di protezione dei dati personali", che d'ora in poi nel presente documento sarà richiamato semplicemente come "Codice";

premesso che:

- ai sensi dell'art.28 del Codice nel presente atto, Titolare dei dati personali trattati da parte di questo Istituto è l'Istituto stesso, di cui il Dirigente Scolastico in carica è Legale Rappresentante;
- il Titolare ha applicato l'art. 29 del Codice che consentiva la facoltà di nominare uno o più Responsabili di tutti o parte dei trattamenti e che pertanto è stato nominato il DSGA dell'Istituto;
- l'art. 30 del Codice impone di nominare gli Incaricati del trattamento dei dati;
- l'art.33 impone di adottare le misure di sicurezza disposte dal Codice e almeno le misure minime individuate dall'allegato B del Codice stesso;

considerato che:

- occorre definire le misure minime di sicurezza, per l'attività di ciascuna unità organizzativa nel trattamento di dati personali e per l'esecuzione di procedimenti amministrativi, e individuare gli Incaricati;
- la nomina a Incaricato non implica l'attribuzione di funzioni ulteriori rispetto a quelle già assegnate bensì soltanto ricevere un'autorizzazione a trattare dati personali e istruzioni sulle modalità cui attenersi nel trattamento;
- l' articolazione organizzativa dell'Istituto è fondata su 5 unità: collaboratori del Dirigente Scolastico, personale docente (compresi docenti esterni ufficialmente incaricati di supplenze temporanee, esami o altre funzioni presso l'Istituto), personale di segreteria, personale ausiliario (collaboratori scolastici) e membri (anche esterni alla scuola) degli Organi Collegiali,

DESIGNANO INCARICATI DEL TRATTAMENTO DEI DATI

1. i "docenti interni", di ruolo o supplenti, assistenti alla didattica, tecnici e personale di sostegno, di volta in volta assegnati all'Istituto;
2. i "docenti esterni" incaricati ufficialmente di funzioni nella scuola (esami, corsi, concorsi e attività integrative), per gli ambiti dei trattamenti sotto specificati:
 - a) ogni dato inerente gli alunni e le rispettive famiglie e la carriera scolastica degli alunni, limitatamente agli aspetti rilevanti e funzionali allo svolgimento della funzione docente ed educativa e finalizzati alla realizzazione dell'offerta formativa, limitatamente agli alunni delle classi a ciascuno affidate o agli alunni che partecipano a progetti o attività, anche integrative e/o complementari, in cui il docente sia coinvolto per progetti o incarichi previsti dal Piano dell'offerta Formativa;
 - b) dati relativi a comunicazioni riservate personali degli alunni e/o delle rispettive famiglie;
 - c) dati relativi alle giustificazioni per le assenze dalle lezioni da parte degli alunni;
 - d) dati relativi ad esperti e/o ditte esterne per quanto riguarda le attività didattiche, integrative e/o complementari per gli alunni, per incarichi organizzativi o funzionali all'offerta formativa dell'istituzione deliberati dal Collegio dei Docenti o su espresso incarico del Dirigente Scolastico.

In particolare ogni Incaricato designato dovrà effettuare il trattamento dei dati di sua competenza attenendosi scrupolosamente alle seguenti modalità:

- 1) effettuare il trattamento in modo lecito e secondo correttezza;
- 2) raccogliere e registrare i dati per gli scopi inerenti l'attività svolta;
- 3) verificare, ove possibile, l'esattezza dei dati e, se necessario, aggiornarli;
- 4) verificare che i dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Responsabile/Titolare;
- 5) rispettare, nella conservazione, le misure di sicurezza predisposte nell'istituzione scolastica; in ogni operazione di trattamento deve essere garantita la massima riservatezza, anche tra colleghi appartenenti a consigli di intersezione, interclasse e classe diversi;

- 6) non far uscire documenti dalla sede scolastica, neanche temporaneamente;
- 7) non fare copie della documentazione salvo autorizzazioni del Responsabile o del Titolare;
- 8) durante il trattamento mantenere i documenti contenenti dati personali fuori dalla portata di vista di terzi anche se dipendenti dell'istituzione;
- 9) al termine del trattamento custodire i documenti all'interno di archivi muniti di serratura o nei locali ad accesso vigilato;
- 10) in caso di allontanamento anche temporaneo del posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'Incaricato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non incaricati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento;
- 11) nessun dato può essere comunicato a terzi o diffuso in qualsiasi forma, anche ad altri dipendenti non incaricati, senza la preventiva specifica autorizzazione del Titolare o del Responsabile;
- 12) le comunicazioni agli interessati contenenti dati personali dovranno avvenire in forma "riservata"; se effettuate per scritto dovranno essere consegnate direttamente all'interessato o in modo che non risultino accessibili i dati in essi contenuti (foglio piegato e spillato o in busta chiusa) tranne quando si tratti di dati pubblici come, per esempio, voti e giudizi riportati dagli alunni nelle prove di profitto di qualsiasi tipo, le valutazioni intermedie e finali,;
- 13) all'atto della consegna di documenti l'Incaricato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta;
- 14) qualsiasi documento o comunicazione "riservata" consegnata o in possesso all'Incaricato non deve essere trattenuta, ma consegnata con urgenza direttamente al Titolare o al Responsabile o farla pervenire loro in busta chiusa con la scritta RISERVATO;
- 15) il possesso delle chiavi pertinenti alla scuola di servizio, implica le responsabilità connesse e deve essere dichiarato per iscritto.

Tutto il personale docente Incaricato è contrattualmente soggetto, anche al di fuori dell'orario di lavoro e anche dopo la cessazione del rapporto stesso, ad osservare il segreto professionale e a non divulgare quindi dati, fatti o informazioni di qualsiasi tipo di cui è venuto a conoscenza nello svolgimento dell'incarico conferito.

DETERMINANO INOLTRE

1. fermi restando obblighi e responsabilità civili e penali dei dipendenti pubblici nell'ambito delle attività d'ufficio, di disporre sotto vincolo disciplinare l'obbligo tassativo di attenersi alle suddette istruzioni per tutti i dipendenti facenti parte dell'unità organizzativa "Docenti";
2. di mettere a disposizione copia del D.L.vo 196/2003 ed altri materiali informativi;
3. di organizzare apposite riunioni esplicative e formative;
4. di mettere a disposizione, non appena redatto, il Documento Programmatico sulla Sicurezza;
5. di consegnare, all'atto dell'assunzione in servizio, a ogni nuovo componente anche temporaneo dell'unità organizzativa in oggetto copia del presente documento e i relativi allegati e di provvedere affinché riceva un'adeguata informazione individuale.

Copia del presente documento, pubblicato all'Albo dell'Istituto, è consegnata ad ogni unità di personale Incaricato. Copia firmata per ricevuta e presa visione è conservata in segreteria.

Il Responsabile del trattamento dati – DSGA
Rag. Maria Teresa Messoriano

IL DIRIGENTE SCOLASTICO
Dott.ssa Maria Paola MINETTI

Il/La sottoscritto/a	_____ cognome e nome del dipendente
nella sua qualità di	_____ qualifica all'interno dell'Istituzione Scolastica
dichiara di aver ricevuto Lettera di incarico: unità organizzativa "docenti" di cui all'art.13 del D.L.vo 196/2003	
_____ luogo e data	_____ firma leggibile

LETTERA DI INCARICO: PERSONALE DI SEGRETERIA

IL DIRIGENTE SCOLASTICO E IL DSGA

visto:

- l’art. 30 del D.L.vo 196/2003 “Codice in materia di protezione dei dati personali”, che d’ora in poi nel presente documento sarà richiamato semplicemente come “Codice”;

premessi che:

- ai sensi dell’art.28 del Codice nel presente atto, Titolare dei dati personali trattati da parte di questo Istituto è l’Istituto stesso, di cui il Dirigente Scolastico in carica è Legale Rappresentante;
- il Titolare ha applicato l’art. 29 del Codice che consentiva la facoltà di nominare uno o più Responsabili di tutti o parte dei trattamenti e che pertanto è stato nominato il DSGA dell’Istituto;
- l’art. 30 del Codice impone di nominare gli Incaricati del trattamento dei dati;
- l’art.33 impone di adottare le misure di sicurezza disposte dal Codice e almeno le misure minime individuate dall’allegato B del Codice stesso;
- che il trattamento dei dati rientra nelle competenze proprie del profilo professionale per ciascuno contrattualmente determinato ed è quindi obbligatorio e necessario per lo svolgimento delle specifiche funzioni;

considerato che:

- occorre definire le misure minime di sicurezza, per l’attività di ciascuna unità organizzativa nel trattamento di dati personali e per l’esecuzione di procedimenti amministrativi, e individuare gli Incaricati;
- la nomina a Incaricato non implica l’attribuzione di funzioni ulteriori rispetto a quelle già assegnate bensì soltanto ricevere un’autorizzazione a trattare dati personali e istruzioni sulle modalità cui attenersi nel trattamento;
- l’ articolazione organizzativa dell’Istituto è fondata su 5 unità: collaboratori del Dirigente Scolastico, personale docente (compresi docenti esterni ufficialmente incaricati di supplenze temporanee, esami o altre funzioni presso l’Istituto), personale di segreteria, personale ausiliario (collaboratori scolastici) e membri (anche esterni alla scuola) degli Organi Collegiali,

DESIGNANO INCARICATI DEL TRATTAMENTO DEI DATI

le unità di personale, di ruolo o supplente, di volta in volta assegnate agli uffici di segreteria, per gli ambiti dei trattamenti sotto specificati:

1. settore didattico: - ogni dato inerente gli alunni e le rispettive famiglie;
 -ogni dato inerente la carriera scolastica degli alunni;
 -dati riguardanti l’orientamento;
 -dati relativi alle ditte esterne per quanto riguarda le attività didattiche e l’attività formativa degli alunni;
2. settore personale : -ogni dato inerente il personale ATA o il personale docente;
 -dati relativi alle graduatorie interne ed esterne degli aspiranti all’impiego presso l’istituzione;
3. protocollo: -ogni corrispondenza o atto in entrata o in uscita dall’istituzione, con l’esclusione del protocollo riservato, anche quando tratti di persone e riguardi dati sensibili;
4. amministrazione: - ogni dato inerente esperti, consulenti, fornitori per tutti gli adempimenti preliminari o conseguenti a contratti per la fornitura di beni e servizi;
 -ogni dato relativo ai dipendenti per quanto riguarda la liquidazione di compensi, le assicurazioni, i contributi e le trattenute fiscali o a qualunque titolo.

L’affidamento dei compiti e dei servizi è suscettibile di eventuali variazioni e di interscambi di unità di personale in caso di

improcrastinabili esigenze di servizio.

In particolare ogni Incaricato designato dovrà effettuare il trattamento dei dati solo di sua competenza e attenersi scrupolosamente alle seguenti modalità:

- 1) effettuare il trattamento in modo lecito e secondo correttezza;
- 2) raccogliere e registrare i dati per gli scopi inerenti l'attività svolta;
- 3) verificare, ove possibile, l'esattezza dei dati e, se necessario, aggiornarli;
- 4) verificare che i dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Responsabile/Titolare;
- 5) in ogni operazione di trattamento deve essere garantita la massima riservatezza, anche tra incaricati non coinvolti nello specifico trattamento o pratica ed in particolare:
 - divieto di comunicazione a terzi e/o diffusione in qualsiasi forma dei dati senza la preventiva autorizzazione del Titolare o del Responsabile;
 - l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
 - la fase di raccolta del consenso dovrà essere preceduta dalla informativa ed il consenso al trattamento dei dati dovrà essere rilasciato in forma scritta;
- 6) rispettare e far rispettare, nella conservazione, le misure di sicurezza predisposte nell'istituzione scolastica;
- 7) non far uscire documenti dalla sede scolastica, neanche temporaneamente;
- 8) non fare copie della documentazione salvo autorizzazioni del Responsabile o del Titolare;
- 9) durante il trattamento mantenere i documenti contenenti dati personali fuori dalla portata di vista di terzi anche se dipendenti dell'istituzione;
- 10) al termine del trattamento custodire i documenti all'interno di archivi muniti di serratura o nei locali ad accesso vigilato;
- 11) in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'Incaricato dovrà verificare che non vi sia la possibilità da parte di terzi, anche se dipendenti non incaricati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento;
- 12) le comunicazioni agli interessati contenenti dati personali dovranno avvenire in forma "riservata"; se effettuate per scritto dovranno essere consegnate direttamente all'interessato o in modo che non risultino accessibili i dati in essi contenuti (foglio piegato e spillato o in busta chiusa), tranne quando si tratti di dati pubblici;
- 13) all'atto della consegna di documenti l'Incaricato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta;
- 14) qualsiasi documento o comunicazione "riservata" consegnata, naturalmente in busta chiusa, all'Incaricato non deve essere trattenuta, ma consegnata con urgenza direttamente al Titolare o al responsabile;
- 15) non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Responsabile;
- 16) Informare il Responsabile in caso di incidente di sicurezza che coinvolga dati sensibili e non;
- 17) rammentare che il possesso delle chiavi pertinenti alla scuola di servizio, implica le responsabilità connesse e deve essere dichiarato per iscritto.

La presente designazione ha validità per l'intero anno scolastico e si intende conferita, di volta in volta, al personale inserito nell'ufficio o nella funzione anche in corso d'anno e viene comunque a cessare al modificarsi del rapporto di lavoro.

Tutto il personale docente Incaricato è contrattualmente soggetto, anche al di fuori dell'orario di lavoro e anche dopo la cessazione del rapporto stesso, ad osservare il segreto professionale e a non divulgare quindi dati, fatti o informazioni di qualsiasi tipo di cui è venuto a conoscenza nello svolgimento dell'incarico conferito.

DETERMINANO INOLTRE

1. fermi restando obblighi e responsabilità civili e penali dei dipendenti pubblici nell'ambito delle attività d'ufficio, di disporre sotto vincolo disciplinare l'obbligo tassativo di attenersi alle suddette istruzioni per tutti i dipendenti facenti parte dell'unità organizzativa "Personale di Segreteria";
2. di mettere a disposizione copia del D.L.vo 196/2003 ed altri materiali informativi;
3. di organizzare apposite riunioni esplicative e formative;
4. di mettere a disposizione, non appena redatto, il Documento Programmatico sulla Sicurezza;
5. di consegnare, all'atto dell'assunzione in servizio, a ogni nuovo componente anche temporaneo dell'unità organizzativa in oggetto copia del presente documento e i relativi allegati e di provvedere affinché riceva un'adeguata informazione individuale.

Copia del presente documento, pubblicato all'Albo dell'Istituto, è consegnata ad ogni unità di personale di segreteria.
Copia firmata per ricevuta e presa visione è conservata in segreteria.

Il Responsabile del trattamento dati – DSGA
Rag. Maria Teresa Messoriano

IL DIRIGENTE SCOLASTICO
Dott.ssa Maria Paola MINETTI

Il/La sottoscritto/a	_____
	cognome e nome del dipendente
nella sua qualità di	_____
	qualifica all'interno dell'Istituzione Scolastica
dichiara di aver ricevuto Lettera di incarico: "personale di segreteria" di cui all'art.13 del D.L.vo 196/2003	
	Per accettazione
_____	_____
luogo e data	firma leggibile

Prot. n. 930/A2

Felizzano, 31.03.2015

LETTERA DI INCARICO: PERSONALE COLLABORATORE SCOLASTICO

IL DIRIGENTE SCOLASTICO E IL DSGA

visto:

- l’art. 30 del D.L.vo 196/2003 “Codice in materia di protezione dei dati personali”, che d’ora in poi nel presente documento sarà richiamato semplicemente come “Codice”;

premessi che:

- ai sensi dell’art.28 del Codice nel presente atto, Titolare dei dati personali trattati da parte di questo Istituto è l’Istituto stesso, di cui il Dirigente Scolastico in carica è Legale Rappresentante;
- il Titolare ha applicato l’art. 29 del Codice che consentiva la facoltà di nominare uno o più Responsabili di tutti o parte dei trattamenti e che pertanto è stato nominato il DSGA dell’Istituto;
- l’art. 30 del Codice impone di nominare gli Incaricati del trattamento dei dati;
- l’art.33 impone di adottare le misure di sicurezza disposte dal Codice e almeno le misure minime individuate dall’allegato B del Codice stesso;
- che il trattamento dei dati rientra nelle competenze proprie del profilo professionale per ciascuno contrattualmente determinato ed è quindi obbligatorio e necessario per lo svolgimento delle specifiche funzioni;

considerato che:

- occorre definire le misure minime di sicurezza, per l’attività di ciascuna unità organizzativa nel trattamento di dati personali e per l’esecuzione di procedimenti amministrativi, e individuare gli Incaricati;
- la nomina a Incaricato non implica l’attribuzione di funzioni ulteriori rispetto a quelle già assegnate bensì soltanto ricevere un’autorizzazione a trattare dati personali e istruzioni sulle modalità cui attenersi nel trattamento;
- l’ articolazione organizzativa dell’Istituto è fondata su 5 unità: collaboratori del Dirigente Scolastico, personale docente (compresi docenti esterni ufficialmente incaricati di supplenze temporanee, esami o altre funzioni presso l’Istituto), personale di segreteria, personale ausiliario (collaboratori scolastici) e membri (anche esterni alla scuola) degli Organi Collegiali,

DESIGNANO INCARICATI DEL TRATTAMENTO DEI DATI

1. le unità di personale collaboratore scolastico, di ruolo o supplente, di volta in volta assegnate ai plessi e/o alle sezioni facenti capo all’Istituto, per gli ambiti dei trattamenti sotto specificati:
 - a) ogni dato inerente i terzi per tutti gli adempimenti conseguenti a contratti per la fornitura di beni o servizi

In particolare ogni Incaricato designato dovrà effettuare il trattamento dei dati solo di sua competenza e attenersi scrupolosamente alle seguenti modalità:

- 1) astenersi dall’effettuare qualsiasi tipo di trattamento di dati esclusi quelli del punto a);
- 2) raccogliere e consegnare con urgenza eventuali dati a lui/lei consegnati per forze di causa maggiore (assenza momentanea Incaricato preposto), pretendendo che vengano inseriti in busta chiusa con l’indicazione dell’Incaricato autorizzato al ritiro e trattamento;
- 3) rispettare e far rispettare, nella conservazione, le misure di sicurezza predisposte nell’istituzione scolastica;
- 4) non far uscire documenti dalla sede scolastica, neanche temporaneamente;
- 5) non fare copie e/o fotocopie di qualsiasi tipo di documentazione (esclusa quella di stretta pertinenza didattica) salvo autorizzazioni del Responsabile o del Titolare ;

- 6) non comunicare a terzi o diffondere in qualsiasi forma dati e/o informazioni di cui si è venuti in possesso, anche casualmente, nello svolgimento del proprio lavoro;
- 7) non tentare di aprire, senza specifica autorizzazione del Titolare o del Responsabile, archivi muniti di serratura o locali ad accesso vigilato;
- 8) qualsiasi documento o comunicazione "riservata", consegnata naturalmente in busta chiusa, non deve essere trattenuta, ma consegnata con urgenza direttamente al Titolare o al Responsabile;
- 9) non modificare le regole e i trattamenti esistenti o introdurne nuovi senza l'esplicita autorizzazione scritta del Responsabile;
- 10) informare il Responsabile in caso di incidente di sicurezza che coinvolga qualsiasi tipo di dati, sensibili e non;
- 11) rammentare che il possesso delle chiavi pertinenti alla scuola di servizio, implica le responsabilità connesse e deve essere dichiarato per iscritto.

La presente designazione ha validità per l'intero anno scolastico e si intende conferita, di volta in volta, al personale inserito nell'ufficio o nella funzione anche in corso d'anno e viene comunque a cessare al modificarsi del rapporto di lavoro.

Tutto il personale Collaboratore Scolastico è contrattualmente soggetto, anche al di fuori dell'orario di lavoro e anche dopo la cessazione del rapporto stesso, ad osservare il segreto professionale e a non divulgare quindi dati, fatti o informazioni di qualsiasi tipo di cui è venuto a conoscenza nello svolgimento dell'incarico conferito.

DETERMINANO INOLTRE

1. fermi restando obblighi e responsabilità civili e penali dei dipendenti pubblici nell'ambito delle attività d'ufficio, di disporre sotto vincolo disciplinare l'obbligo tassativo di attenersi alle suddette istruzioni per tutti i dipendenti facenti parte dell'unità organizzativa "Personale Collaboratore Scolastico";
2. di mettere a disposizione copia del D.L.vo 196/2003 ed altri materiali informativi;
3. di organizzare apposite riunioni esplicative e formative;
4. di mettere a disposizione, non appena redatto, il Documento Programmatico sulla Sicurezza;
5. di consegnare, all'atto dell'assunzione in servizio, a ogni nuovo componente anche temporaneo dell'unità organizzativa in oggetto copia del presente documento e i relativi allegati e di provvedere affinché riceva un'adeguata informazione individuale.

Copia del presente documento, pubblicato all'Albo dell'Istituto, è consegnata ad ogni unità di personale Collaboratore Scolastico. Copia firmata per ricevuta e presa visione è conservata in segreteria.

Il Responsabile del trattamento dati – DSGA
Rag. Maria Teresa Messoriano

IL DIRIGENTE SCOLASTICO
Dott.ssa Maria Paola MINETTI

Il/La sottoscritto/a	_____ <small>cognome e nome del dipendente</small>
nella sua qualità di	_____ <small>qualifica all'interno dell'Istituzione Scolastica</small>
dichiara di aver ricevuto Lettera di incarico: "personale collaboratore scolastico" di cui all'art.13 del D.L.vo 196/2003	
_____ <small>luogo e data</small>	_____ <small>firma leggibile</small>



ISTITUTO COMPRENSIVO "G. PASCOLI"
di Scuola dell'Infanzia, Primaria e Secondaria di I Grado
P.zza Paolo Ercole, 6 – 15023 Felizzano (AL)
Tel. 0131-791122 sel. 2 – FAX 0131-791395 CF: 96034370062
www.icpascoli-felizzano.gov.it – e-mail: icpascoli-felizzano@libero.it

Documento programmatico sulla sicurezza (ai sensi del D.L.vo n.196 del 30.06.03)

MODELLO "Riservatezza" per e-mail in uscita

****** Riservatezza******

In ottemperanza al D.Lgs. n. 196 del 30/6/2003 in materia di protezione dei dati personali, le informazioni contenute in questo messaggio sono strettamente riservate ed esclusivamente indirizzate al destinatario indicato (oppure alla persona responsabile di rimmetterlo al destinatari).

E' vietato l'uso, la diffusione, distribuzione o riproduzione da parte di ogni altra persona.

Nel caso in cui aveste ricevuto questo messaggio di posta elettronica per errore, siete pregati di segnalarlo immediatamente al mittente e distruggere quanto ricevuto (compreso i file allegati) senza farne copia.

Qualsiasi utilizzo non autorizzato del contenuto di questo messaggio costituisce violazione dell'obbligo di non prendere cognizione della corrispondenza tra altri soggetti, salvo più grave illecito, ed espone il responsabile alle relative conseguenze.

IL DIRIGENTE SCOLASTICO
Dott.ssa Maria Paola MINETTI

ISTITUTO COMPRENSIVO “G. PASCOLI”
di Scuola dell’Infanzia, Primaria e Secondaria di I Grado
P.zza Paolo Ercole, 6 – 15023 Felizzano (AL) - CF96034370062
Tel.0131-791122 sel. 2 – FAX 0131-791395
www.icpascoli-felizzano.gov.it

email: icpascoli-felizzano@libero.it – alic81800q@istruzione.it – PEC: alic81800q@pec.istruzione.it

AL DIRIGENTE SCOLASTICO
ISTITUTO COMPRENSIVO “G. PASCOLI”
DI FELIZZANO

OGGETTO: LETTERA LIBERATORIA PER L’UTILIZZO DI IMMAGINI (foto o filmati) A
TITOLO GRATUITO.

Con la presente i sottoscritti _____
genitori dell’alunno/a _____ frequentante la Scuola
(Infanzia/Primaria/Secondaria di I grado) _____

_____ di _____ autorizzano l’Istituto Comprensivo “G.
Pascoli” di Felizzano ad utilizzare, per manifestazioni e/o concorsi scolastici, eventuali lavori
realizzati a scuola dai Docenti in cui sono presenti fotografie e/o videoregistrazioni con l’immagine
del proprio figlio/a e dichiarano di non avere nulla a pretendere per dette prestazioni.

Inoltre, in conformità del D.lvo 196/03, (1) non autorizzano/ autorizzano l’utilizzo per la
pubblicazione sul sito web dell’Istituto www.icpascoli-felizzano.gov.it della foto del proprio
figlio/a a soli scopi didattici e culturali.

Dichiarano inoltre di esprimere, in ordine ai contenuti della Legge sulla privacy (DL. 675/96), il
consenso all’utilizzo dei dati personali ai sensi dell’art. 13 1. cit. per l’intera durata della
permanenza dell’alunno nell’I.C. di Felizzano, fino a comunicazione scritta di revoca
dell’autorizzazione.

In fede.

Felizzano, _____

Firma

Madre _____

Padre _____

Tutor legale _____
(se esistente)

(1) Cancellare la voce che non interessa