REPUBBLICA ITALIANA - REGIONE SICILIANA
ISTITUTO COMPRENSIVO STATALE "SAN PIERO PATTI"(ME)
Via Profeta 27

***98068 San Piero Patti (Me)* – Tel. e Fax. 0941.661033**
Cod. Mecc. MEIC878001 – Cod. Fisc. 94007180832
E-mail: meic878001@istruzione.it

REGOLAMENTO D' ISTITUTO IN MATERIA DI PRIVACY

Anno Scolastico 2014/2015

INDICE

PREMESSA

Il presente regolamento disciplina il trattamento dei dati personali in attuazione del Testo Unico sulla Privacy, D.Lgs. 30/06/2003 n.196.

1. FINALITA'

Il presente regolamento ha lo scopo di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
Le disposizioni che regolano la materia della privacy sono finalizzate anche a ridurre al minimo i rischi di sottrazione, distruzione o perdita, anche accidentale, dei dati personali mediante l'adozione di idonee e preventive misure di sicurezza, costantemente adeguate nel tempo.

2. DEFINIZIONI DI RIFERIMENTO

Ai fini del presente regolamento, per le definizioni si rinvia, in via prevalente, a quanto previsto dall'art. 4, comma 1, del D.Lgs. 196/03:
a) "trattamento", qualunque operazione o complesso di operazioni, effettuati 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 di dati, anche se non registrati in una banca di dati;
b) "dato personale", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;
d) "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;
e) "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 articoli 60 e 61 del codice di procedura penale;
f) "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in

ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
g) "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
i) "interessato", la persona fisica cui si riferiscono i dati personali;
l) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
m) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
n) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
o) "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
p) "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
q) "Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

3. DIRITTI DELL'INTERESSATO

L'interessato ha diritto di conoscere l'utilizzo dei dati che lo riguardano ed in particolare può opporsi all'uso degli stessi per attività diverse da quella oggetto dell'operazione che attua con l'Istituto, secondo quanto previsto dall'art.7 del Codice della Privacy.

4. SOGGETTI E RESPONSABILITÀ

Titolare del trattamento
Quando il trattamento è effettuato da una persona fisica, da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.
Nella fattispecie, si identifica il Titolare del trattamento nella persona del procuratore del Dirigente Scolastico pro-tempore.

Responsabile del trattamento
Il responsabile può essere designato dal titolare del trattamento. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni impartitegli, tramite apposita lettera di incarico.
Nella fattispecie, si identificano come Responsabili del trattamento un Docente, facente parte dello staff di dirigenza, ed il Direttore SGA.

Incaricati del trattamento
Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. La designazione

è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Gli incaricati possono accedere solo ai dati strettamente pertinenti alla collaborazione richiesta.
Nella fattispecie, sono identificati quali incaricati tutti gli addetti dell'area amministrativa/di segreteria e dell'area docente.

Custode delle credenziali di autenticazione
Quando vi è più di un incaricato del trattamento e sono pertanto in uso più credenziali di autenticazione (user id e password), viene nominato per iscritto un soggetto preposto alla conservazione delle credenziali di autenticazione, che ha accesso ad informazioni che concernono le medesime. Potrà trattarsi dello stesso titolare o del responsabile del trattamento, se nominato.
Il custode delle credenziali di autenticazione sarà nominato con apposita lettera.
Nella fattispecie, è individuato quale custode delle credenziali di autenticazione il docente dell'area informatica o un impiegato dell'area amministrativa.

Amministratore di sistema
L'Amministratore di Sistema è assunto dal Provvedimento a carattere generale del Garante Privacy 27.11.2008 quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, quali le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.
Nella fattispecie, è individuato quale Amministratore di Sistema il docente dell'area informatica o tecnica o un impiegato dell'area amministrativa – in ultima analisi anche soggetto esterno.

5. INFORMATIVA

L'interessato o la persona presso la quale sono raccolti i dati personali saranno previamente informati per iscritto circa:
a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei dati medesimi;
e) i diritti di cui all'articolo 7 del D.Lgs.196/03;
f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 D.Lgs.196/03 e del responsabile.
Se i dati personali non sono raccolti presso l'interessato, l'informativa comprensiva delle categorie di dati trattati, sarà data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.
Nella fattispecie, l'informativa specifica viene fornita, con la contestuale acquisizione del consenso:
- agli studenti ed alle loro famiglie, all'atto della prima iscrizione all'Istituto;
- al personale dipendente e collaboratori (docenti, personale amministrativo e di segreteria, personale ausiliario) all'atto dell'instaurazione del rapporto;
- ad eventuali terzi per attività collegate al funzionamento dell'Istituto e per attività culturali e ricreative (ex studenti e operatori vari), prima dell'inizio delle attività stesse.

6. TRATTAMENTO DEI DATI

Si assicura che i dati personali oggetto di trattamento saranno:
a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
c) esatti e, se necessario, aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
Si assicura inoltre che:
a) ogni documento, sia cartaceo sia informatico, sarà usato solo ed esclusivamente per adempiere ad obblighi di legge o previsti dal contratto posto in essere;
b) fermi restando gli obblighi relativi alla sicurezza, il trattamento dei dati sarà effettuato con logiche e banche dati strettamente correlate e funzionali agli obblighi, ai compiti o alle finalità contemplate dall'autorizzazione.
In caso di cessazione, per qualsiasi causa, di un trattamento i dati saranno: i;
a) riconsegnati all'interessato – se richiesti;
c) conservati per fini esclusivamente istitutzionali e non destinati ad una comunicazione sistematica o alla diffusione.
Il trattamento dei dati è effettuato dall'Istituto sia con modalità informatiche, sia con modalità cartacee.

Relativamente alla prima modalità, è stato introdotto il Registro elettronico, contenente tutte le informazioni attinenti gli studenti, utilizzato dal personale docente e di segreteria e reso disponibile alle famiglie mediante accesso web, protetto con credenziali di accesso individuali. (1)

Relativamente alla seconda modalità, tutte le informazioni relative al rendimento scolastico degli alunni, i giustificativi delle assenze, la documentazione contenente dati sensibili (stato di salute, orientamento religioso, ecc..) e giudiziari, sono conservati nel Fascicolo dello studente, conservato nell'Ufficio di Segreteria I documenti di carattere amministrativo sono conservati negli Uffici di segreteria e amministrazione.
La documentazione relativa al personale ed a terzi per attività culturali e ricreative promosse dall'Istituto è trattata con modalità cartacea dall'Ufficio di Segreteria.
La documentazione relativa a ex studenti e operatori vari è trattata con modalità cartacee dall'Ufficio di Segreteria.
Con particolare riferimento a situazioni specifiche, l'Istituto ha adottato le seguenti prescrizioni:

TEMI IN CLASSE: nell'eventualità in cui gli elaborati, contenenti argomenti delicati, vengano letti in classe, ogni docente incaricato dovrà adottare l'adeguato equilibrio tra le esigenze didattiche e la tutela dei dati personali.
Restano comunque validi gli obblighi di riservatezza già previsti per il corpo docente riguardo al segreto d'ufficio e professionale, nonché quelli relativi alla conservazione dei dati personali eventualmente contenuti nei temi degli alunni.

VOTI SCOLASTICI, SCRUTINI, TABELLONI, ESAMI DI STATO: per il principio di trasparenza, a garanzia di ogni studente, i voti degli scrutini e degli esami sono pubblicati nell'Albo dell'Istituto, avendo attenzione a non fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti o altri dati personali non pertinenti.

CIRCOLARI E COMUNICAZIONI SCOLASTICHE: nell'ambito delle attività di informazione alle famiglie sugli avvenimenti della vita scolastica, l'Istituto evita ogni riferimento che permetta di risalire anche indirettamente all'identità degli studenti coinvolti in vicende particolarmente delicate.

ORIENTAMENTO, FORMAZIONE E INSERIMENTO LAVORATIVO: previo consenso degli studenti interessati, l'Istituto comunica a terzi (enti, associazioni, imprese pubbliche e private) i dati relativi ai loro risultati scolastici, al fine di promuovere attività di orientamento, formazione e inserimento lavorativo, anche all'estero.

FOTO DI CLASSE, RIPRESE VIDEO: le riprese video e le fotografie possono essere effettuate solo per le finalità istituzionali (didattiche, culturali, ricreative), a seguito di autorizzazione dei Presidi di ogni ciclo scolastico e del consenso dei soggetti interessati o di chi esercita la patria potestà.
Le registrazioni delle lezioni sono effettuate solo da personale incaricato, per motivi di studio. In caso di diffusione è necessario acquisire il consenso degli interessati.
Sono assolutamente vietate le riprese audio-video, anche se effettuate da telefoni cellulari, all'interno delle aule di lezione e nella scuola stessa, da parte di studenti. La violazione di tale prescrizione, violando il diritto alla riservatezza delle persone riprese, comporterà sanzioni disciplinari interne, qualora non si configuri anche una più grave fattispecie di reato.

CELLULARI E TABLET L'uso di cellulari è in genere consentito per fini strettamente personali, (ad esempio per registrare le lezioni), e sempre nel rispetto delle persone. Non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. E' bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati. (***)

LE GRADUATORIE La pubblicazione sui siti Internet degli istituti delle graduatorie di docenti e personale amministrativo tecnico
e ausiliario (Ata) per consentire a chi ambisce a incarichi e supplenze di conoscere la propria posizione e punteggio. Tali liste, giustamente accessibili a tutti, non devono però contenere, come in diversi casi segnalati al Garante, i numeri di telefono e gli indirizzi privati dei candidati. Questa illecita diffusione dei contatti personali incrementa, tra l'altro, il rischio di esporre i lavoratori a forme di stalking o a possibili furti di identità. Le graduatorie di vario tipo, non debbono contenere dati personali non pertinenti o eccedenti le finalità istituzionali perseguite.

TABLET E SMARTPHONE A SCUOLA Nuove tecnologie e web rappresentano ormai una realtà con cui fare i conti anche nell'ambito dell'attività scolastica. Smartphone e tablet sono utili, ad esempio, per registrare le lezioni o per fare ricerche. Ma non devono trasformarsi in strumenti di offesa usandoli per diffondere sulla rete video e foto che possono ledere la dignità di compagni o insegnanti.

7. SICUREZZA

I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato, o di trattamento non consentito o non conforme alle finalità della raccolta.
In riferimento all'allegato B del Testo Unico sulla Privacy, sono adottate le seguenti misure minime di sicurezza:
a) autenticazione informatica, con specifica password richiesta all'avvio del computer;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;(3)

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un documento interno, aggiornato in merito alle misure di sicurezza adottate. (4)

Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici, prevede le seguenti misure minime di sicurezza:
a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati;
b) adozione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti (archivi muniti di sistemi di chiusura per impedire l'accesso da parte di terzi estranei, con relativo controllo da parte del personale incaricato, lacerazione dei documenti da eliminare).

8. RESPONSABILE DEL TRATTAMENTO

Il responsabile del trattamento provvede a:
- individuare e nominare per iscritto gli incaricati del trattamento, impartendo loro, sempre per iscritto, le idonee istruzioni;
- vigilare sul rispetto delle istruzioni impartite agli incaricati;
- adottare e rispettare le misure di sicurezza indicate e predisposte dal titolare del trattamento;
- individuare i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
- verificare trimestralmente lo stato di applicazione del D.Lgs. 30 giugno 2003 n. 196, nonché il buon funzionamento, la corretta applicazione e la conformità alle indicazioni dell'Autorità Garante dei sistemi e delle misure di sicurezza adottate;(5)
- evadere tempestivamente tutte le richieste e gli eventuali reclami degli interessati;
- interagire con i soggetti incaricati di eventuali verifiche, controlli o ispezioni;
- comunicare immediatamente al titolare gli eventuali nuovi trattamenti da intraprendere nel proprio settore di competenza, provvedendo alle necessarie formalità di legge;
- conservare i dati personali in caso di cessazione del trattamento degli stessi, provvedendo alle necessarie formalità di legge.

9. INCARICATI DEL TRATTAMENTO

Gli incaricati del trattamento hanno accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati.
In particolare gli incaricati devono:
a) trattare tutti i dati personali di cui vengono a conoscenza nell'ambito dello svolgimento delle proprie funzioni, in modo lecito e secondo correttezza;
b) utilizzare la parola chiave richiesta all'avvio del computer;
c) sostituire autonomamente la parola chiave trimestralmente, previa comunicazione al soggetto preposto alla custodia;
d) utilizzare il codice identificativo e la parola chiave per il trattamento dei dati su elaboratore quando connesso in rete;
e) evitare di creare banche dati nuove senza espressa autorizzazione del titolare (o del responsabile);
f) evitare di asportare supporti informatici o cartacei contenenti dati di terzi, senza la previa autorizzazione del titolare (o del responsabile);

g) conservare i documenti, eventualmente prelevati dall'archivio, nei cassetti della propria scrivania dotati di serratura. Nei periodi in cui la scrivania rimarrà incustodita, tali cassetti dovranno rimanere chiusi e la chiave dovrà rimanere in possesso dell'incaricato;
h) riporre nell'archivio, immediatamente dopo il loro utilizzo, i documenti prelevati dallo stesso e richiuderlo a chiave;
i) identificare e registrare i soggetti che vengono ammessi agli archivi dopo l'orario di chiusura.

10. PIANO DELLE VERIFICHE

A cura del responsabile del trattamento sono periodicamente attivati controlli, anche a campione, al fine di garantire la sicurezza e l'attendibilità dei dati trattati.
Durante queste operazioni sarà data particolare importanza alla verifica di:
- adeguatezza delle misure di antintrusione adottate;
- correttezza dell'utilizzo delle parole chiave e dei profili di accesso degli incaricati e la loro modifica;
- disattivazione dei codici di accesso non utilizzati per più di sei mesi;
- aggiornamento dei dispositivi antivirus;
- aggiornamento dei i programmi software che trattano i dati personali;
- integrità dei dati e delle loro copie di back up;(6)
- adeguatezza nella conservazione dei documenti cartacei;
- distruzione dei supporti magnetici che non possono più essere riutilizzati;
- aggiornamento dell'ambito del trattamento consentito ai singoli incaricati;
- livello di formazione degli incaricati ed eventuale programmazione di sessioni di aggiornamento, anche in relazione all'evoluzione tecnica e tecnologica avvenuta in azienda.

Di queste verifiche sarà redatto un apposito verbale.

11. PIANO DI FORMAZIONE

Il piano di formazione rivolto agli incaricati verte sui seguenti argomenti:
- norme per la tutela dei dati personali e misure minime di sicurezza, aspetti legislativi e operativi;
- gestione delle credenziali di autenticazione e norme per la loro custodia;
- regolamentazione dei rapporti con l'incaricato della custodia delle credenziali;
- cautele da osservare per assicurare la segretezza delle credenziali e la custodia dei dispositivi di autenticazione;
- norme di gestione dello strumento informatico durante e fuori dalle sessioni di trattamento;
- controllo e custodia di atti e documenti cartacei.

Almeno una volta l'anno, verrà istituito un incontro per sensibilizzare gli incaricati sull'importanza di adottare le norme di sicurezza predisposte e per recepire eventuali suggerimenti in materia, derivanti dalla constatazione della presenza di minacce o vulnerabilità riscontrate.

CAPO II: UTILIZZO DEL SISTEMA INFORMATICO

Premessa
1. Utilizzo dello strumento informatico
2. Gestione delle credenziali di autenticazione
3. Utilizzo della rete
4. Utilizzo di pc portatili
5. Uso della posta elettronica
6. Uso della rete internet e dei relativi servizi

PREMESSA

L'utilizzo delle risorse informatiche e telematiche sia da parte del personale dipendente (docenti, personale amministrativo e di segreteria), sia da parte degli studenti deve sempre ispirarsi al principio della diligenza e correttezza, trattandosi per gli uni di uno strumento di lavoro e per gli altri di uno strumento di apprendimento.
L'Istituto ha adottato un regolamento interno, diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

1. UTILIZZO DELLO STRUMENTO INFORMATICO

Ogni utilizzo del personal computer da parte del personale dipendente o di studenti, non inerente all'attività lavorativa o formativa, può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza del sistema informatico.
L'accesso allo strumento informatico è consentito tramite credenziali di autenticazione (user id e password).
Non è consentito installare autonomamente programmi provenienti dall'esterno, in quanto sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni software.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente.
L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Istituto a gravi responsabilità civili e anche penali, in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
Non è consentito all'utente di modificare la configurazione predefinita del proprio strumento informatico.
Il personal computer deve essere spento alla fine di ogni sessione di trattamento.
Non è consentita l'installazione sul proprio strumento informatico di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.).
L'utilizzo di supporti di origine esterna deve essere autorizzato dal Titolare sentito l'Amministratore di Sistema.

2. GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE

Le credenziali di autenticazione necessarie all'accesso al sistema informativo, sia singoli pc, sia rete, consistono in un codice per l'identificazione dell'incaricato (user id), associato ad una parola chiave riservata (password), conosciuta solamente dall'utente.
Le password di ingresso alla rete e di accesso ai programmi sono attribuite dagli utenti. È necessario procedere alla modifica della password al primo utilizzo e, successivamente, almeno ogni trei mesi.

La password soddisfa i requisiti di complessità, componendosi di almeno otto caratteri (lettere maiuscole, minuscole, simboli e numeri), essendo priva di senso compiuto e non direttamente riconducibile all'utente.
E' vietato comunicare a terzi la propria password di accesso, così come trascriverla in modo da renderla visibile a chiunque ed è necessario custodirla con la massima diligenza.
I tentativi di accesso al sistema informativo sono limitati a tre: gli utenti che digiteranno la propria password in modo errato e ripeteranno in successione l'errore altre due volte, saranno automaticamente disabilitati e, quindi, verrà loro revocata la possibilità di accedere al sistema stesso. Il ripristino sarà a cura dell'Amministratore di Sistema (7).
La custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente, per iscritto, il soggetto incaricato alla loro custodia (Custode delle credenziali di autenticazione).
Il custode delle credenziali di autenticazione potrà accedere ai dati ed agli strumenti informatici esclusivamente per garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività dell'Istituto, nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente lo stesso dell'intervento di accesso realizzato.
Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, così come in caso di perdita della qualità che consente all'incaricato l'accesso ai dati.

3. UTILIZZO DELLA RETE

Le unità di rete sono aree di condivisione di informazioni dell'Istituto e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e back up.
Le procedure di back up sono effettuate in conformità a quanto previsto al punto 18 del disciplinare tecnico – Allegato B D.Lgs. n.196/2003. (8)
È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
L'Amministratore di Sistema può, in qualunque momento, procedere alla rimozione di ogni file o applicazione che ritenga essere pericoloso per la sicurezza, sia sui pc degli incaricati, sia sulle unità di rete.
Costituisce buona regola la periodica pulizia degli archivi, con cancellazione dei files obsoleti o inutili (files temporanei, svuotamento del cestino esistente sul desk top, ecc.), da effettuarsi almeno ogni tre mesi. (9)
Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
E' del pari opportuno effettuare la scansione completa del sistema con l'antivirus in dotazione ogni volta che si rileva una situazione critica e, comunque, almeno una volta al mese. (10)
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

4. UTILIZZO DI PC O ALTRA STRUMENTAZIONE PORTATILE

L'utente è responsabile della strumentazione portatile assegnatagli e deve custodirla con diligenza, sia durante gli spostamenti, sia durante l'utilizzo nell'Istituto.
Agli strumenti portatili si applicano le regole di utilizzo previste per gli strumenti connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso, prima della riconsegna.
Gli strumenti portatili utilizzati all'esterno devono essere custoditi in un luogo protetto.

Quando per la connessione in rete si utilizza un sistema wi-fi, si dovranno utilizzare apposite credenziali di accesso, atte a proteggere la rete stessa.(11)

5. USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata dall'Istituto all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
E' obbligatorio inserire, in chiusura di ogni mail inviata, la dicitura di conformità del trattamento al D.Lgs. n. 196/2003.
È obbligatorio utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.
È vietato inviare catene telematiche.

6. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Gli strumenti elettronici abilitati alla navigazione in internet costituiscono uno strumento necessario allo svolgimento della attività istituzionali e didattiche. È assolutamente proibita la navigazione in internet per motivi diversi da quelli sopra definiti.
È fatto divieto all'utente di scaricare software gratuito (freeware) e shareware prelevato da siti internet.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività istituzionale.
È vietata la partecipazione a forum non professionali, blog, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).
Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari, nonché con le azioni civili e penali consentite.

Il Titolare del Trattamento

APPENDICE

(1) Detto paragrafo dovrà essere attenzionato e se necessario integrato.
(2) Detto paragrafo va lasciato inserito se ci sono sistemi di video sorveglianza.
(3) (4) Si ricorda tenuta registro reporter.
(5) Verbali periodici – trimestrali.
(6) Si ricorda tenuta registro reporter.
(7) Questo paragrafo dovrà restare inserito se il sistema di password e tarato come descritto, altrimenti dovrà essere riformulato.
(8) Si ricorda tenuta registro reporter.
(9) Pulizia File obsoleti amm.re sistema o altro soggetto - Trimestrale – Verbale specifico.
(10) Verificare se si effettua la scansione Virus mensile , altrimenti adeguare paragrafo.
(11) Stumentazione portatile seguirà casistica pc rete – Verificare – ed eventualmente correggere e modificare.
(***) Spetta comunque agli istituti scolastici decidere nella loro autonomia come