MINISTERO DELL'ISTRUZIONE DELL'INIVERSITA' E DELLA RICERCA
Direzione didattica 1° Circolo
V.le S. Dell'Uomo, 44
20081 Abbiategrasso

Abbiategrasso 3 marzo 2011 ***Prot. N°308/B37***

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI PERSONALI

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

DISPOSIZIONI MINIME SULLA SICUREZZA

E

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente documento si compone di n. 13 pagine (inclusa la presente)

Il titolare
(Dr. Sebastiano Grande)

_____

Aggiornamento 3 marzo 2011 prot. N°308/B37

OGGETTO E AMBITO DI APPLICAZIONE

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica della segreteria della Direzione Didattica 1° Circolo e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

La rete della Direzione Didattica 1° Circolo è connessa alla rete Internet.

I provvedimenti organizzativi e le misure adottate sono finalizzate a 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*."

Il documento è redatto dal Dirigente scolastico Grande Sebastiano al fine di mettere in atto le misure di sicurezza per tutelare i dati personali oggetto del trattamento, predisporre e adottare le misure di sicurezza organizzative, fisiche e logiche ed è così articolato:

Definizioni

Titolare del trattamento dei dati: persona giuridica cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, anche in ordine alla adozione di misure minime di sicurezza;

responsabile del trattamento dei dati: persona preposta dal titolare al trattamento di dati personali;

incaricati: persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

amministratore di sistema: soggetto che sovrintende alle risorse di rete e ne consente l'utilizzazione;

custode delle password: soggetto cui è conferita la gestione delle password degli incaricati del trattamento dei dati;

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

dati personali: informazioni relative 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 articoli 60 e 61 del codice di procedura penale.

Art 1 Descrizione del Sistema Informatico

Il sistema informatico del 1° Circolo Didattico è costituito dai seguenti componenti:

Hardware

- Esiste una rete LAN "Segreteria" (1 SERVER e 7 PC multimediali negli uffici)
- Il Server utilizza il sistema operativo "WINDOWS 2000";
- Oltre ai PC già elencati, esistono n° 4 stampanti di rete,
- connessione verso l'esterno: n° 1 router ADSL. per tutti i i PC facenti parte della rete LAN
- A valle del router principale ADSL, esiste un sistema firewall hardware su sistema operativo.

Software

- Tutti i PC funzionano con sistema operativo WINDOWS 'XP;
- Le applicazioni di tipo gestionale utilizzate sono le seguenti:
- Per tutte le aree amministrative: AXIOS;
- Per il protocollo: AXIOS;
- Per i libri di testo: AXIOS;
- Applicazioni di office (Office 2010 e XP Standard e professional);
- Sistemi di posta elettronica: strumenti di navigazione in Internet: Internet explorer;
- Posta elettronica certificata

Art. 2 Elenco dei trattamenti dei dati

Tabella 1

Descrizione sintetica del Trattamento		Natura dei dati trattati	Struttura di riferimento	Altre strutture che concorrono al trattamento	Descrizione degli strumenti utilizzati
Attività svolta	interessati				
Gestione Personale	**Personale docente, A.T.A.; Collaboratori ed esperti**	**Dati personali**	**Segreteria**	**Centro servizi amministrativi; INPS, INPDAP, MIUR**	**Personal Computer in rete, Internet; armadi**
Gestione alunni	**Alunni, famiglie**	**Dati Personali, Dati sensibili**	**Segreteria**	**Centro servizi Amministrativi, Anagrafe Nazionale, Scuole sec. I°**	**Personal Computer in rete, Internet; armadi**

Art. 3 Descrizione della struttura

Tabella 2 - Descrizione della struttura organizzativa dell'Istituto

Struttura	Trattamenti effettuati sulla struttura	Descrizione dei compiti e delle responsabilità della struttura
Segreteria amministrativa	Retribuzione, compensi, adempimenti fiscali, erariali, previdenziali, Anagrafe prestazioni, Ricostruzione carriera, Attestazioni e Certificazioni, assenze.	**Acquisizione dati e caricamento, consultazione, comunicazione a terzi; salvataggio**
Segreteria Didattica	**Certificazioni, assenze, anagrafe, Consultazione;**	**Acquisizione dati e caricamento, consultazione, comunicazione a terzi; salvataggio**

Art. 4 Personale incaricato del trattamento in ogni strutura e delle dotazioni informatiche

Nome e cognome	Struttura di riferimento	Strumenti utilizzati	Responsabilità aggiuntive
Enrica Portaluppi,	**Segreteria**	**PC n° PS7PRC010370-6133332701**	
Marisa Santangelo	**Segreteria**	**PC n° PS7PRC010370-5A8812701**	
Paola Manetta	**Segreteria**	**PC n° PS680E6306647-0429EL00**	
Domenica Bossoni	**Segreteria**	**PC n° PS7PRC010370-50A88B2701**	
Rosalia Panebianco	**Segreteria**	**PC n° TM25155225C20598**	
M.Luisa Rosina	**Segreteria**	**PC n° FGXZ420351174**	
M.Luisa Rosina	**Segreteria**	**PC n° 105080D100**	
M.Luisa Rosina	**Segreteria**	**TTG32100160500DC8EL00**	**Backup Custodia P.W.**

Art. 5 Connettività internet

Connettività	Apparecchiature di comunicazione	Provider
ADSL	**ROUTER**	**Telecom**

Art.5 Descrizione Personal Computer [1]

	Identificativo di PC	Tipo PC	Sistema operativo	Software utilizzato	rete
1	PC n° PS7PRC010370-6133332701	Acer veriton 7900	WINDOWS XP	OFFICE , SISSI	SI
2	PC n° PS7PRC010370-5A8812701	Acer veriton 7900	WINDOWS XP	OFFICE , SISSI	SI
3	PC n° PS680E6306647-0429EL00	Acer veriton 6800	WINDOWS XP	OFFICE , SISSI	SI
4	PC n° PS7PRC010370-50A88B2701	Acer veriton 7900	WINDOWS XP	OFFICE , SISSI	SI
5	PC n° TM25155225C20598	*Asus*	WINDOWS XP	OFFICE , SISSI	SI
6	PC n° FGXZ420351174	*LG*	WINDOWS XP	OFFICE , SISSI	SI
7	PC n° 105080D100	Generico	WINDOWS XP	OFFICE , SISSI	
8	TTG32100160500DC8EL00	Acer Altos G320	WINDOWS 2003	SISSI	SI

[1] I PC descritti in questa tabella **non** prendono in considerazione quelli presenti nei laboratori didattici

Art. 6
MISURE DI CARATTERE ELETTRONICO/INFORMATICO

Le misure di carattere elettronico/informatico[2] adottate sono:

- utilizzo di server con configurazioni di ridondanza *(attiva)*;
- presenza di gruppi di continuità elettrica per il server *(attiva)*;
- attivazione di un sistema di backup centralizzato e automatizzato con periodicità settimanale e storico di un mese *(attiva)*. Alla data di questo documento i responsabili delle copie sono indicati nell'Allegato 1 relativo al censimento dei trattamenti dei dati;
- installazione di un firewall con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet;
- definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows XP, di seguito specificate *(misura attiva)*;
- divieto di memorizzare dati personali, sensibili, giudiziari sulle postazioni di lavoro con sistemi operativi Windows 9x e Windows Me;
- installazione di un sistema antivirus su tutti le postazioni di lavoro, configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico con frequenza settimanale e la scansione periodica dei supporti di memoria *(misura attiva SYMANTEC);*
- definizione delle regole per la gestione di strumenti elettronico/informatico, di seguito riportate;
- definizione delle regole di comportamento per minimizzare i rischi da virus, di seguito riportate*;*
- separazione della rete locale della segreterie da laboratori didattici *(attiva)*.

[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.

Art. 7
REGOLE PER LA GESTIONE DELLE PASSWORD[3]

Le assistenti amministrative incaricate del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato user-id) e password personale.
User-id (costituita da nome.cognome) sono assegnati dal custode delle password;
Password (composta da 8 caratteri alfanumerici)
User-id e password sono strettamente personali.
La 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 sei mesi (tre nel caso di trattamento dati sensibili) 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 tre mesi di non utilizzo.
Le password di amministratore di tutti i PC che lo prevedono sono assegnate dall'amministratore di sistema, esse 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 possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. 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

- le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo;
- per la definizione/gestione della password devono essere rispettate le seguenti regole:
  - la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
  - *deve contenere almeno un carattere alfabetico ed uno numerico;*
  - *non deve contenere più di due caratteri identici consecutivi;*
  - *non deve contenere lo user-id come parte della password;*
  - al primo accesso la password ottenuta dal custode delle password deve essere cambiata; *la nuova password non deve essere simile alla password precedente;*
  - la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
  - *la password termina dopo sei mesi di inattività*;
  - la password è segreta e non deve essere comunicata ad altri;
  - la password va custodita con diligenza e riservatezza;
  - l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia.

[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.

Art. 8 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 *cassetta* sono conservate in armadio metallico
- *divieto di utilizzare floppy disk come mezzo per il backup*;
- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. *A tale riguardo, per evitare errori e dimenticanze, è adottato uno screensaver automatico dopo 10 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.*
- *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.

Il fax si trova in locale ad accesso controllato *(segreteria)* e l'utilizzo è consentito unicamente alle assistenti amministrative, alla D.S.G.A.
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.

Art. 9 REGOLE DI COMPORTAMENTO PER MINIMIZZARE I RISCHI DA VIRUS[4]

Per ridurre rischi da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- utilizzare esclusivamente gli applicativi autorizzati
- 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 senza determinare 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

Art. 10 ANOMALIE E RIPRISTINO[5] INCIDENT RESPONSE

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente 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(vedi tabella 3).

Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso[6];

1 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 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 (vedere Allegato 2) il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto.

Procedure di spegnimento

Sistema operativo	Azione
Windows 98/NT/2003/XP	1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Staccare la spina dalla presa di corrente.

[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.

Art. 11 MINACCE

Rrisorse hardware
Le principali minacce alle risorse hardware sono:
malfunzionamenti dovuti a guasti; a eventi naturali quali terremoti, allagamenti, incendi; blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica; sabotaggi, furti, intercettazioni (apparati di comunicazione).

Risorse connesse in rete
Le principali minacce alle risorse connesse in rete possono provenire dall'interno dell'istituto, dall'esterno o da una combinazione interno/esterno e sono relative:
all'utilizzo della LAN/Intranet (interne);
ai punti di contatto con il mondo esterno attraverso Internet (esterne);
allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interne/esterne).

Articolo 12
PRINCIPI GENERALI – DIRITTI E RESPONSABILITÀ

La Direzione Didattica 1° Circolo promuove l'utilizzo della rete quale strumento per il perseguimento di finalità istituzionali.
Il personale amministrativo consapevole delle potenzialità offerte dagli strumenti informatici e telematici si impegna 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.

Articolo 13
ABUSI E ATTIVITÀ VIETATE

E' 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;
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne limitino l'utilizzabilità e le prestazioni per altri utenti;
- 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; 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 del 1° Circoloper scopi 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;
- lasciare la postazione di lavoro incustodita o accessibile, come specificato nell'allegato 3.

Articolo 14
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;

Articolo 15
SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE

Hanno diritto ad accedere alla rete della Direzione Didattica 1° Circolo il personale ATA 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'amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.

Articolo16
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 ogni altra altre norma che disciplina l'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 17
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 dal CCNL.