Istituto Comprensivo Statale "C. Goldoni"
Villaverla - Montecchio Precalcino
(Vicenza)

Via Giovanni XXIII, n. 9 – 36030 Villaverla tel.: 0445-350244 - fax:0445-350234 – www.icvillaverla.it
Contatti:e-mail: segreteria@icvillaverla.it (Segreteria); dirigente@icvillaverla.it (Dirigente);VIIC81100D@pec.istruzione.it (Posta Certificata)

PUA

Politica d'Uso Accettabile delle Tecnologie dell'informatica e della Comunicazione della Scuola

Testo approvato dal Consiglio di Istituto con delibera n 6 del 12.02.2014

PUA

Politica d'Uso Accettabile e sicuro della Rete

INTRODUZIONE

Un gruppo di lavoro, su incarico del Dirigente Scolastico, ha elaborato questo documento sulla Politica d'Uso Accettabile della rete. La PUA fa parte delle strategie delle T.I.C. e si basa su linee guida delle politiche nazionali.
Il documento è revisionato su base annuale per adeguarsi alle trasformazioni ed innovazioni tecnologiche e normative.

CONTENUTI

1. I vantaggi derivanti dall'uso della rete e della connessione ad Internet
2. Analisi dei rischi
3. Strategie dell'Istituto per garantire la sicurezza delle T.I.C.
4. I gestori della rete d'Istituto
5. Il regolamento per l'utilizzo della rete

Allegati: Modulo per richiesta di Identificativo Utente e di assunzione di responsabilità per il personale

1- I VANTAGGI DERIVANTI DALL'USO DELLA RETE E DI INTERNET

I vantaggi per la didattica ed in generale per la gestione complessiva delle risorse informatiche derivanti dalla disponibilità della rete sono molteplici; alcuni sono elencati di seguito:

a) Condivisione di risorse hardware come stampanti e hard disk
b) Disponibilità dei propri documenti ed impostazioni in modo indipendente dalla stazione di lavoro a cui ci si connette
c) Sicurezza dei dati memorizzati su server con hardware ridondante
d) Possibilità di distribuire in modo immediato materiale didattico
e) Accesso a data base centralizzati per le attività didattiche ed amministrative
f) Collegamento alla rete Internet
g) Posta elettronica sia esterna che interna
h) Pubblicazione del sito dell'Istituto con possibilità di accedere a materiali didattici anche dall'esterno (e-learning)
i) Erogazione di corsi on-line

Il collegamento alla rete Internet, in particolare, offre agli studenti ed al personale della scuola la possibilità di accedere ad uno sterminato archivio di informazioni e quindi si pone come mezzo di eccellenza per promuovere l'attitudine al continuo aggiornamento, stimolare curiosità costruttive, reperire documentazione altrimenti non facilmente accessibile, effettuare scambi culturali con altre persone, perfezionare le competenze nelle lingue straniere (in particolare l'inglese).
In seconda istanza, su Internet sono facilmente reperibili immense raccolte di software freeware e open source in grado di risolvere praticamente qualsiasi problema applicativo a costo zero, nel pieno rispetto della legalità e della normativa sulla proprietà intellettuale.
A tutti i vantaggi elencati in precedenza si associano comunque anche alcuni rischi, derivanti sia da cause interne che esterne; questi rischi vanno accuratamente analizzati e per ognuno di essi occorre prendere le opportune contromisure per annullarli o, quantomeno, minimizzarli.

2-L'ANALISI DEI RISCHI

I rischi connessi all'uso della rete si possono raggruppare nelle seguenti categorie:

- Perdita di dati, eventualmente sensibili
- Diffusione di malware (virus informatici, Trojan Horse, worm, backdoors e simili)
- Abusi da utenti interni verso l'interno
- Abusi da utenti interni verso l'esterno (Internet o altre reti raggiungibili mediante connessioni VPN)
- Abusi da utenti esterni verso l'interno
- Download di materiale illegale o protetto dalla normativa sul diritto d'autore

- Accesso a siti monitorati dall'autorità giudiziaria, inadatti alla visione da parte di minorenni ed in ogni caso di contenuto moralmente condannabile
- Abusi nell'utilizzo della posta elettronica
- Rischi connessi all'uso improprio di chat room e di forum non moderati
- Violazioni della normativa sulla privacy

Fermo restando che nessuna struttura informatica sarà mai in grado di annullare completamente questi rischi, la loro riduzione ad avvenimenti sporadici ed in ogni caso controllabili deve avvenire mediante quattro strade diverse ma fra di loro complementari:

I. Informazione
II. Controllo
III. Prevenzione
IV. Repressione

I. L'informazione è responsabilità dei docenti che lavorano normalmente in aule computerizzate, dotate di LIM (Lavagna Interattiva Multimediale) o in laboratori, con il supporto eventuale dell'amministratore di rete e dai suoi collaboratori. Essa si applica a tutte le categorie di rischio elencate in precedenza, ad eccezione della perdita di dati e degli abusi da esterno a interno.

II. Il controllo è anch'esso una responsabilità dei docenti e viene favorito dalla condotta del singolo nella gestione e nell'utilizzo degli strumenti (PC, LIM), dal rispetto degli orari di accesso ai laboratori, dall'abitudine ad un modo di lavoro preciso ed ordinato.

III. La prevenzione si esplica essenzialmente con l'utilizzo di opportune contromisure tecnologiche messe in atto dall'amministratore di rete.

IV. La repressione degli abusi da interno verso interno passa attraverso le normali procedure delle sanzioni disciplinari. Gli abusi da interno verso esterno sono invece di pertinenza dei Carabinieri, della Polizia Postale e della Guardia di Finanza.

3-STRATEGIE PER RIDURRE I RISCHI E MIGLIORARE LA SICUREZZA

L'informazione agli utenti

L'informazione viene erogata agli utenti mediante un approccio gerarchico. L'amministratore di rete, su delega del Dirigente, provvede a inizio anno ad illustrare ai docenti ed al personale in servizio nell'Istituto i punti fondamentali che riguardano la gestione della sicurezza informatica. I docenti devono farsi carico di trasmettere queste informazioni ai loro allievi. In generale, gli utenti devono diventare coscienti dei rischi connessi alla navigazione su Internet e devono essere educati al rispetto delle normative interne ed alla collaborazione con il personale tecnico di gestione per segnalare tempestivamente attività illecite che eventualmente sfuggano ai sistemi di controllo automatici predisposti dall'amministratore.

In modo particolare devono essere sottolineati ed evidenziati i seguenti punti:

- ✓ Evitare, nel modo più assoluto, di fornire su Internet il proprio recapito o anche solo la località di residenza. Non diffondere su Internet proprie fotografie;
- ✓ Usare sempre dei nickname di fantasia, non riconducibili al proprio vero nome;
- ✓ Registrarsi con nome ed email solo su siti individuabili senza il minimo dubbio;
- ✓ In caso di accesso fortuito a siti evidentemente illegali (pedofilia, ad esempio), sfuggiti al filtro Internet, disconnettersi immediatamente ed avvertire l'amministratore fornendo l'URL del sito oppure quello della pagina Web che ha condotto al sito in esame, in modo tale che esso possa essere immediatamente inserito nella black list. E' necessario spiegare chiaramente agli utenti che questi siti sono monitorati dalla Polizia Postale e che un accesso reiterato può significare l'iscrizione ad una lista di persone da indagare
- ✓ Scegliere password di accesso alla rete non banali e non comunicarle ad altri, neppure agli insegnanti, per nessun motivo. Il nome utente e la relativa password costituiscono infatti il metodo con cui viene identificata la persona che ha fatto accesso alla rete.
- ✓ In caso di allontanamento dalla propria postazione di lavoro, bloccare la workstation in modo tale che un altro utente non possa commettere abusi con le nostre credenziali

Il controllo dell'attività degli utenti

Il controllo dell'attività degli studenti è un preciso obbligo del personale docente, da esercitare in modo particolarmente attento quando queste attività si svolgono in laboratorio. Per garantire una sorveglianza ottimale è necessario rispettare le seguenti regole:

- ✓ **Rispetto dell'orario**: ogni laboratorio ha un orario affisso sulla porta d'ingresso, con l'indicazione della classe e dei docenti che hanno diritto ad occuparlo nelle varie ore.
- ✓ **Etichettatura dei PC**: ogni computer deve essere dotato di una etichetta, chiaramente leggibile e non facilmente asportabile o deteriorabile, su cui è segnato il nome del PC. Tale nome è composto da un prefisso, coincidente con la sigla del laboratorio, un trattino ed una numerazione progressiva. Ad esempio, il primo computer del laboratorio di Informatica è identificato dal nome "alunni1". Questo nome è identico a quello che è stato assegnato alla macchina durante l'installazione del sistema operativo e che viene registrato nei file di log dei server. In questo modo è possibile tracciare non solo l'utente ma anche la macchina su cui è stato commesso un eventuale abuso.
- ✓ **Firma del registro per segnalare eventuali malfunzionamenti**: (SOLO SCUOLA SEC.di 1° Gr.) ogni laboratorio è dotato di un registro in cui il docente che rilevasse eventuali malfunzionamenti apporrà la propria firma. Anche ogni allievo, nel caso trovi qualcosa che non va, anche di piccola entità, deve immediatamente avvertire il docente e segnalare il danno riscontrato.
  E' altresì indispensabile che nel laboratorio non possano assolutamente circolare studenti privi di sorveglianza, neppure per brevi periodi di tempo.
- ✓ **Permanenza nel tempo sulla postazione di lavoro**: nei limiti del possibile, è necessario fare in modo che un determinato studente occupi sempre la stessa postazione di lavoro. In questo modo si facilita l'individuazione degli abusi relativi agli accesi con credenziali altrui, si riducono le probabilità di danneggiamenti volontari alle attrezzature e si occupa meno spazio sul disco fisso per la memorizzazione dei profili locali.

La prevenzione dei rischi

Come già detto, la prevenzione è un compito che spetta all'amministratore di rete. Egli la mette in atto ricorrendo ad opportune tecnologie hardware/software, dettagliate in questo paragrafo in riferimento ai rischi elencati in precedenza.

- ✓ **Perdita di dati**: il rischio di perdere dati a seguito di un malfunzionamento hardware o software viene affrontato essenzialmente con l'uso delle cartelle remote e con il backup regolare
- ✓ **Diffusione di malware**: su tutti i server e su ogni PC della rete è installato un sistema antivirus. A complemento del sistema antivirus, le workstation sono dotate di software antispyware, anch'esso soggetto ad aggiornamenti periodici. Sulle macchine collegate alle LIM è stato installato un firewall software per il filtraggio dei siti web (black list). Il controllo sui worm che si diffondono soprattutto mediante e-mail infette viene affrontato consentendo agli studenti la lettura della posta esclusivamente mediante Web Mail. Il personale degli uffici, che possiede invece client di tipo POP3, è stato opportunamente istruito circa l'opportunità di aprire solo la posta di cui conosce il mittente, cestinando quella sospetta. In ogni caso, il nostro provider Internet possiede un filtro abbastanza efficace sui suoi server, in grado di filtrare anche una buona percentuale di spam.
- ✓ **Abusi da utenti interni verso l'interno (Area uffici Amministrativi)**: questi abusi si riconducono essenzialmente ai tentativi di intrusione nelle cartelle remote di altri utenti, al fine di cancellare o modificare i loro documenti, oppure a quelli di accedere a condivisioni su server riservate ai docenti o al personale degli uffici. Questo rischio viene controllato mediante un'attenta politica delle password. A tal fine si è fatto ricorso ad opportune "group policies" configurate sul controller di dominio che gestisce l'ambiente Active Directory. Le regole imposte sulle password sono le seguenti:
    - La password ha una durata massima di novanta giorni
    - La password deve rispondere a requisiti di complessità: quando l'utente la sceglie, il server controlla che essa sia lunga almeno otto caratteri e che comprenda al suo interno almeno tre delle seguenti caratteristiche:
        - Caratteri maiuscoli
        - Caratteri minuscoli
        - Numeri
        - Simboli speciali

Per migliorare ulteriormente la sicurezza, specie in relazione ai dati sensibili eventualmente conservati dalla segreteria, è stata separata la rete amministrativa da quella didattica.
Un altro tipo di abuso interno consiste nel tentativo, da parte degli studenti, di installare sulle macchine software non autorizzato. Questo tentativo viene efficacemente contrastato dal sistema operativo stesso, che non consente agli utenti privi di privilegi amministrativi l'installazione di alcun tipo di software. Risulta invece più complesso impedire l'utilizzo di software non ammesso (in prevalenza giochi) che non richiede installazione e che può essere lanciato a partire da supporti rimovibili (chiavette USB, CD-ROM). Il controllo di questo tipo di abuso è quindi affidato ai docenti in servizio che hanno il dovere di monitorare l'attività dei loro studenti e di riferire all'amministratore o ai suoi collaboratori il nome dei programmi utilizzati senza autorizzazione; in questo caso è infatti possibile un efficace controllo centralizzato mediante regole imposte tramite Group Policies.

- ✓ **Abusi da utenti interni verso l'esterno**: si tratta dei classici attacchi informatici, volti a forzare la protezione di reti remote appartenenti ad aziende, enti privati o governativi e istituzioni di vario tipo, per penetrare all'interno delle loro basi dati, carpire password di utenti di tali reti o danneggiare la loro infrastruttura, oppure destinati ad impossessarsi di numeri di carta di credito, coordinate bancarie di conti correnti eccetera. Rientrano in questa categoria anche gli attacchi DoS (Denial of Service) diretti a bloccare o rallentare l'attività di server remoti per danneggiare, ad esempio, siti di e-commerce. Si tratta di abusi assai gravi, perseguibili penalmente, ma per fortuna anche molto difficili da portare a termine in quanto richiedono competenze informatiche ben superiori alla norma. Questo rischio viene minimizzato dalle regole di accesso ad Internet poste in essere dal firewall e dal filtro installato su di esso, il quale impedisce l'accesso a siti in cui si trovano istruzioni per compiere questo genere di violazioni e limita inoltre l'uso di protocolli di comunicazione non standard. Anche in questo caso, comunque, gioca un ruolo essenziale la sorveglianza del docente il quale deve impedire che uno studente passi ore di fronte al PC senza sapere che cosa esattamente sta facendo.
- ✓ **Abusi da utenti esterni verso l'interno**: questo rischio viene efficacemente controllato e praticamente annullato dal firewall che protegge la rete interna. Per migliorare la protezione da attacchi esterni, il sistema operativo di ogni PC o server viene aggiornato in modo automatico con le più recenti *patch* di sicurezza.
- ✓ **Download di materiale illegale**: il problema si pone particolarmente in relazione all'uso dei programmi di connessione P2P (Peer To Peer). La maggior parte di questi programmi si può lanciare direttamente da una chiavetta USB e non abbisogna di installazione. La limitazione all'uso di questi software è molto difficile, dato che restano attivi in background e quindi non sono controllabili da un'ispezione visiva. L'amministratore ha comunque attivato tutta una serie di accorgimenti che, nella maggior parte dei casi, impediscono il lancio di questi programmi o ne limitano pesantemente le funzionalità. Dato però che i client P2P sono molto numerosi e nuove versioni sono continuamente proposte su Internet, il controllo al 100% non sembra possibile. Gli utenti devono quindi essere informati che esiste una legge che prevede conseguenze penali per la cessione a terzi di materiale protetto dalla normativa sul diritto d'autore, che nessun software P2P consente il puro download (soggetto solo a sanzioni amministrative) ma, al contrario, il materiale scaricato viene automaticamente messo a disposizione di terze persone e che, infine, non esiste in rete il concetto di anonimato; ogni attività è sempre e comunque tracciabile.
- ✓ **Accesso a siti monitorati dall'autorità giudiziaria**: questo rischio viene quasi annullato dall'azione del filtro Internet installato sul firewall. In ogni caso, la frequentazione di questi siti dev'essere volontaria e ripetuta con regolarità perché possano verificarsi conseguenze spiacevoli come l'iscrizione ad una lista di persone sospette. L'accesso casuale ad uno di questi siti, magari in seguito all'attivazione di un link su una pagina Web, non comporta conseguenze. E' importante, tuttavia, che la cosa venga segnalata tempestivamente all'amministratore che provvederà ad inserire i siti in esame nella *black list* del firewall ed eventualmente a segnalarne l'esistenza all'autorità competente.
- ✓ **Abusi nell'utilizzo della posta elettronica**: i rischi legati all'uso della posta elettronica si possono suddividere in due categorie: da interno ad esterno e viceversa. Gli utenti possono, ad esempio, utilizzare la Web Mail per inviare messaggi contenenti insulti, minacce o calunnie, oppure unire ai messaggi allegati contenenti malware di vario tipo. Si tratta di un abuso da interno ad esterno, praticamente impossibile da limitare con misure tecnologiche, dato che l'uso della Web Mail non è distinguibile da una normale navigazione sul Web. Anche in questo caso l'unica contromisura consiste nell'informazione agli utenti circa le conseguenze anche penali derivanti da questa attività e circa la tracciabilità della loro navigazione su Internet. Per quanto riguarda gli abusi da esterno ad interno possiamo distinguere le seguenti categorie:

- ***Phishing***
- ***Spam***
- ***Catene di S. Antonio***
- ***Diffusione di malware***

Il ***Phishing*** consiste nell'invio di mail contenenti un rimando ad una pagina Web che simula alla perfezione la home page ad esempio di una banca on line, ed in cui si richiede magari di inserire il proprio numero di conto corrente oppure quello della carta di credito. Queste informazioni vengono poi usate dal mittente della mail per scopi truffaldini.

Lo ***Spam*** consiste nell'invio massiccio di posta indesiderata contenente in genere pubblicità di vario tipo, non sempre relativa a prodotti legalmente acquistabili.

Le ***catene di S. Antonio***, spesso legate alle cosiddette "leggende metropolitane" sono messaggi in cui si presenta una situazione tragica, relativa in genere a problemi di salute di bambini, ed in cui si chiede un aiuto economico e l'invio del messaggio stesso a tutti i propri conoscenti.

Il ***malware*** è un termine che raggruppa tutti i software dannosi, non solo virus, worm o trojan ma anche i cosiddetti *spyware* consistenti in programmi che si installano all'insaputa dell'utente, spesso nascosti all'interno di utilities apparentemente innocue, e che una volta in azione monitorizzano continuamente l'attività dell'utente, inviando informazioni, spesso anche dati sensibili, al server del pirata informatico.

La difesa contro il *pishing* è delegata principalmente al buon senso dell'utente, il quale dovrebbe sapere che banche, assicurazioni ed altri enti finanziari non usano le mail per chiedere informazioni riservate ai loro clienti; occorre inoltre considerare che difficilmente uno studente è titolare di carte di credito o conti bancari. La difesa contro lo *spam* è affidata ai filtri *anti spam*, i quali sono gestiti dal provider di servizi Internet. Questi filtri, pur non essendo del tutto efficaci, riescono comunque ad eliminare circa il 90% della posta indesiderata. Dalle *catene di S. Antonio* ci si può difendere semplicemente mediante una ricerca su Internet utilizzando i cosiddetti siti *anti bufala*; è sufficiente digitare una parte del messaggio per sapere se si tratta di una truffa o di un autentico appello. La difesa contro il *malware*, infine, viene svolta efficacemente dal programma antivirus e da programmi *anti spyware.*

- ✓ **Rischi connessi all'uso improprio di chat room:** l'uso delle chat room senza prendere precauzioni conduce a rischi legati essenzialmente a violazione della propria privacy e a diffusione di *malware*. Del secondo problema si è già parlato in diverse occasioni; per quanto riguarda le violazioni della privacy, esse sono di stretta responsabilità dell'utente che non dovrebbe mai *chattare* usando il suo vero nome e soprattutto mai fornire indirizzo, numero di telefono e quant'altro, dato che non si sa mai chi c'è dall'altra parte del filo. In ogni caso, il filtro Internet installato sul firewall blocca la quasi totalità dei siti di *chat*, in quanto essi non hanno in genere validità didattica. L'unica eccezione è costituita da certi *forum* di discussione moderati, che spesso sono decisamente interessanti anche sotto l'aspetto didattico. In questi casi, su richiesta degli utenti, l'amministratore può concedere l'accesso a queste pagine, limitando però il tempo che gli studenti possono usare per la consultazione.

  ✓ **Violazioni della normativa sulla privacy**: questa violazione può avvenire per trasmissione a terzi, senza l'autorizzazione del soggetto interessato, di informazioni testuali o multimediali. Gli utenti della rete non devono comunicare a nessuno, tanto meno su Internet, dati personali di compagni, docenti o personale della scuola in genere e neppure devono riprendere, con telecamere, telefoni cellulari o macchine fotografiche, i soggetti di cui sopra, salvo espresso consenso da parte di un soggetto maggiorenne. E' assolutamente vietato diffondere su Internet filmati realizzati di nascosto durante le lezioni o le altre attività della scuola mediante telefonini o altre apparecchiature dotate di telecamera. Contro questi abusi non esistono prevenzioni tecnologiche attuabili ed anche i controlli sui telefonini sono di scarsa utilità, dal momento che telecamere e macchine fotografiche digitali si trovano ormai integrate su moltissime apparecchiature portatili (computer palmari, PDA, lettori di MP3). Le sole possibilità di approccio al problema consistono nell'informare gli utenti del fatto che queste azioni costituiscono un illecito punibile per legge e nella conseguente repressione.

4. I GESTORI DELLA RETE D'ISTITUTO

Gli amministratori di rete dell'istituto sono i docenti incaricati di Funzione strumentale dell'Area Informatica – Prof. Ugo Barbieri e Prof. Luigi Ceola, coadiuvati dalla Ditta di assistenza informatica "CoverUp" di Sandrigo. La gestione del sito Web è affidata al Dirigente Scolastico dott. Roberto Polga.

All'amministratore sono affidate le seguenti mansioni:

- ✓ Progettare la struttura complessiva della rete sotto l'aspetto delle infrastrutture hardware
- ✓ Installare e mantenere efficienti i sistemi operativi server
- ✓ Installare e mantenere i vari servizi di interesse generale (DHCP, DNS)
- ✓ Configurare gli account utente e provvedere alla loro manutenzione nel tempo
- ✓ Configurare gli account computer
- ✓ Progettare e realizzare la struttura logica di Active Directory, definendo le unità organizzative ed i gruppi di protezione
- ✓ Progettare ed implementare le group policies da applicare ad utenti e computer
- ✓ Configurare i vari servizi di aggiornamento automatico (antivirus, WSUS, antispyware, filtro internet)
- ✓ Controllare il buon funzionamento di tutti i sistemi ed intervenire in modo tempestivo per ripristinarli in caso di errori
- ✓ Controllare il funzionamento del filtro Internet, aggiornare le white list e le black list, applicare le restrizioni in base ai diversi gruppi di utenti
- ✓ Scrivere e mantenere aggiornata la documentazione riguardante il funzionamento della rete, documentando gli interventi fatti
- ✓ Intervenire presso il provider di servizi Internet in caso di problemi
- ✓ Organizzare e controllare le condivisioni su server
- ✓ Fornire supporto agli uffici e ai docenti

5. IL REGOLAMENTO PER L'UTILIZZO DELLA RETE E DI INTERNET

Art. 1
Oggetto e ambito di applicazione

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica dell'Istituto Comprensivo Statale "Carlo Goldoni" di Villaverla - Montecchio Precalcino e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire. La rete dell'Istituto Comprensivo Statale "Carlo Goldoni" di Villaverla - Montecchio Precalcino è connessa alla rete Internet.

Art. 2
Principi generali - diritti e responsabilità

L'Istituto Comprensivo Statale "Carlo Goldoni" di Villaverla - Montecchio Precalcino 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.
Gli utenti sono consapevoli che, essendo la World Wide Web una rete di informazioni non regolamentata, che permette l'accesso ad idee, informazioni ed immagini, l'Istituto non può garantire l'accuratezza delle informazioni nella World Wide Web, né può assumersi alcuna responsabilità per contenuti a cui un utente possa accedere inavvertitamente.
L'Istituto inoltre non si assume alcuna responsabilità per danni, perdite, costi o spese derivanti direttamente o indirettamente dall'uso dei servizi informatici e di consultazione Internet.
Consci 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 dal personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni. Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto vivamente sconsigliato apportare modifiche o installare qualsiasi programma da parte dell'utente o di altri operatori.

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.

Art.3

Abusi e attività vietate sulla rete interna

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

1) Usare la rete in modo difforme da quanto previsto dal presente regolamento.
2) Usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative.
3) Utilizzare la rete per scopi incompatibili con l'attività istituzionale dell'istituto
4) Utilizzare una parola chiave a cui non si è autorizzati.
5) Cedere a terzi codici personali di accesso al sistema.
6) Conseguire l'accesso non autorizzato a risorse di rete interne
7) Violare la riservatezza di altri utenti o di terzi.
8) Agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti.
9) Agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori).
10) Fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati,ecc).
11) Installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi; come, a titolo esemplificativo, virus, cavalli di troia, worms.
12) Installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali.
13) Cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali.
14) Installare deliberatamente componenti hardware non compatibili con le attività istituzionali.
15) Rimuovere, danneggiare deliberatamente o asportare componenti hardware.
16) Utilizzare le risorse hardware e software e i servizi disponibili per scopi personali.
17) 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.
18) Inserire o cambiare la password del B.I.O.S., se non dopo averla espressamente comunicata all'Amministratore di sistema ed essere stati espressamente autorizzati.
19) Abbandonare il posto di lavoro senza bloccare o spegnere l'elaboratore o senza disconnettersi.

Art. 4

Abusi e attività vietate su Internet

1) Conseguire l'accesso non autorizzato a risorse di rete esterne
2) Utilizzare la posta elettronica con la parola chiave di altri utilizzatori.
3) Utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi. L'Istituto non può assumersi alcuna responsabilità per qualsiasi comunicazione ricevuta o spedita da detentori di conti personali di posta elettronica (es.GMail,Hotmail, Msn,etc.).
4) Utilizzare l'accesso ad Internet per scopi personali.
5) Accedere direttamente ad Internet con modem collegato al proprio posto di lavoro, senza utilizzare la connessione autorizzata tramite LAN, se non espressamente autorizzati e per particolari motivi tecnici.
6) Connettersi ad altre reti senza autorizzazione.
7) Usare l'anonimato o servirsi di risorse che consentano di restare anonimi.
8) Installare o eseguire deliberatamente programmi destinati a scaricare materiale illegale o a sovraccaricare sistemi remoti, come ad esempio programmi di file sharing (P2P) o spamming della posta elettronica.

Art. 5

Abusi e attività vietate nei laboratori

Gli utenti non possono:

1) Usare le postazioni di lavoro come base per conseguire l'accesso non autorizzato alle reti o sistemi informatici d'Istituto a qualsiasi altra rete o sistema informatico
2) Fare qualsiasi tentativo di danneggiare apparecchi informatici o software
3) Fare qualsiasi tentativo di alterare la configurazione di software in modo doloso
4) Fare qualsiasi tentativo di degradare le prestazioni del sistema
5) Usare qualsiasi postazione di lavoro dell'Istituto a fini illegali o criminali

Art. 6

Attività consentite

E' consentito all'Amministratore di sistema:

1) 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 e degli studenti.
2) Creare, modificare, rimuovere o utilizzare qualunque parola chiave, 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 e degli studenti.
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 e degli studenti.
4) 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 e degli studenti.

Art. 7

Soggetti che possono avere accesso alla rete

Hanno diritto ad accedere alla rete di istituto tutti i dipendenti, gli studenti, le ditte fornitrici di software per motivi di manutenzione. 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 e di studio, ne devono fare uso.

Art. 8

Modalità di accesso alla rete e agli applicativi

L'utente che ottiene l'accesso alla rete e agli applicativi è impegnato ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed è impegnato 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.

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

Per l'accesso alla rete e agli applicativi, l'utente deve rispettare le seguenti norme:

1) La parola chiave è segreta e non deve essere comunicata ad altri.
2) La parola chiave va custodita con diligenza e riservatezza, in quanto stabilisce un rapporto biunivoco, che permette di responsabilizzare l'incaricato stesso.

3) La parola chiave deve essere costituita da una sequenza di almeno otto caratteri alfanumerici e non deve essere facilmente individuabile.
4) L'utente deve sostituire la parola chiave, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia, come in caso di rivelazione volontaria per specifici motivi.

Art. 9

Trattamento dei dati personali

Tutti gli utenti devono essere consapevoli che le attività svolte sulla rete, ed in particolare quelle su Internet, sono continuamente monitorate in automatico mediante file di "log" giornalieri generati dal firewall. L'amministratore è quindi in grado di conoscere, nel dettaglio, tutti i siti visitati da ogni utente nonché il preciso istante (*timestamp*) in cui è avvenuta questa visita.
Dal momento che questa conoscenza può indirettamente rivelare dati sensibili relativi all'utente, l'amministratore si impegna a rispettare nel modo più rigoroso la corrente normativa sulla privacy. In particolare si impegna a non divulgare a terze persone questi dati ed a conservarne le copie in luogo sicuro ed accessibile solo a lui ed al personale tecnico incaricato espressamente del backup e del restore sui server.
Si informano tuttavia gli utenti che le autorità di pubblica sicurezza, come ad esempio i carabinieri o la polizia postale, possono richiedere la consegna di questi dati a seguito di abusi svolti su Internet di qualsiasi tipo e natura essi siano, la cui origine possa essere fatta risalire senza possibilità di errore alla rete di Istituto. A titolo di esempio si citano:

- invio di e-mail o SMS contenenti ingiurie, minacce, calunnie, ricatti.
- reiterata visita a siti posti sotto il controllo della polizia postale, in particolare siti di pedopornofilia.
- download di materiale sottoposto alla normativa sul diritto d'autore
- attacco informatico verso reti di aziende o altri enti

L'utente della rete interna responsabile di questi abusi verrà identificato mediante i file di log, ne consegue quindi l'importanza del rispetto assoluto dei punti elencati all'Art. 3, in particolare quelli riguardanti la cessione ad altre persone della propria password o l'abbandono anche per brevi intervalli della propria postazione di lavoro senza aver provveduto a bloccarla.

Art. 10

Sanzioni

In caso di abuso, a seconda della gravita 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 interni dell'Istituto.

Villaverla, 12/02/2014

I Referenti dell'Area Informatica di Istituto
- Prof. Ugo Barbieri
- Prof.LuigiCeola

IL DIRIGENTE SCOLASTICO
- Dott. Roberto Polga