Istituto Comprensivo Statale "C. Ederle"
C.so Fraccaroli, 58 – 37049 Villa Bartolomea (VR)
Tel. 0442/659903 - **Fax** 0442/659909 – **Sito**: www.icvillabartolomea.it
e-mail: vric84600r@istruzione.it - **PEC**: icvillabartolomea@pec.icvillabartolomea.it

REGOLAMENTO

PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI

RIFERIMENTO: anno scolastico 2010 – 2011

SOMMARIO

PREMESSA

L'Istituto partendo dall'assunto che l'utilizzo delle risorse informatiche e telematiche presenti al suo interno debba sempre ispirarsi al principio della diligenza e correttezza, adotta un Regolamento diretto a promuovere un utilizzo ottimale dei mezzi a disposizione assicurando efficienza e sicurezza per tutti gli utenti.

CAPO I - FINALITÀ - AMBITO DI APPLICAZIONE – PRINCIPI GENERALI

Art. 1 - Finalità

Il presente regolamento è diretto a definire le norme di accesso e utilizzo degli strumenti informatici, della rete informatica e telematica e dei servizi che tramite la stessa rete è possibile ricevere all'interno e all'esterno dell'Amministrazione, ai fini di un corretto utilizzo degli strumenti stessi da parte degli amministratori, dipendenti e collaboratori di tutto l'Istituto.

L'Amministrazione promuove ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati dell'Istituto.

Art. 2 - Oggetto e ambito di applicazione

La rete dell'Istituto Comprensivo Statale di Villa Bartolomea è costituita dall'insieme delle risorse informatiche, cioè dalle risorse infrastrutturali e dal patrimonio informativo digitale.

Le risorse infrastrutturali sono le componenti hardware/software e gli apparati elettronici collegati alla rete informatica comunale.

Il patrimonio informativo è l'insieme delle banche dati in formato digitale e in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

Il presente regolamento si applica a tutti gli utenti Interni ed Esterni che sono autorizzati ad accedere alla rete comunale.

Per utenti interni s'intendono tutti gli amministrativi, il dirigente, i docenti, i dipendenti a tempo indeterminato e determinato, i collaboratori coordinati e continuativi e il personale con altre forme di rapporto di lavoro.

Per utenti Esterni s'intendono: le ditte fornitrici di hardware e software che eseguono attività di manutenzione limitatamente alle applicazioni di loro competenza, enti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle stesse, collaboratori esterni.

Art. 3 - Principi generali – diritti e responsabilità

L'Istituto Comprensivo Statale di Villa Bartolomea promuove l'utilizzo della Rete Informatica e Telematica, di Internet e della Posta Elettronica quali strumenti utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in accordo con le linee guida e i principi delineati dalla normativa vigente.

Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle Risorse Informatiche, dei servizi/programmi cui ha accesso e dei dati trattati a fini istituzionali. E' altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della

normativa per la tutela dei dati personali. Sono vietati comportamenti che possono creare un danno, anche d'immagine, all'Istituto.

Il presente regolamento considera i divieti posti dallo Statuto dei lavoratori sul controllo a distanza (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 legge 20 maggio 1970, n.300), rispettando durante i trattamenti i principi di necessità (art. 3 del Codice; par. 5.2), correttezza (art. 11, comma 1, lett. a) e finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b del Codice par. 4 e 5).

Per motivi di sicurezza e protezione dei dati, ogni attività compiuta nella Rete Informatica è sottoposta a registrazione in appositi file e riconducibili ad un account di rete. Detti file possono essere soggetti a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo e possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente. La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal D.Lgs. n. 196/2003.

A tutela del dipendente, qualora l'Istituto decidesse di perseguire, per fini legati alla sicurezza dell'intero sistema informativo, il controllo della posta e della navigazione in internet, prima di iniziare il trattamento comunicherà gli strumenti e i modi di trattamento effettuati. Tale compito sarà demandato ad una società esterna a garanzia e tutela delle informazioni di carattere personale dei lavoratori subordinati.

L'Amministratore di Sistema cura l'attuazione del presente regolamento attraverso la predisposizione di Procedure Operative che saranno diffuse tra tutti i dipendenti.

Tali procedure e il presente regolamento sono resi facilmente e continuativamente disponibili per consultazione sui normali mezzi di comunicazione all'interno della struttura.

CAPO II - CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 4 - Utilizzo del personal computer

Il personal computer è uno strumento di lavoro e il suo utilizzo deve essere finalizzato esclusivamente allo svolgimento delle attività professionali e istituzionali dell'Amministrazione.

In particolare:

a. L'accesso all'elaboratore deve essere protetto da password che deve essere custodita dall'Amministratore di Sistema con la massima diligenza e non divulgata. La password deve essere attivata per l'accesso alla rete, per lo screensaver e per il software applicativo. Non è consentita l'attivazione della password di accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema;
b. L'Amministratore di Sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, avrà la facoltà di accedere in qualunque momento anche da remoto (dopo aver richiesto l'autorizzazione all'utente interessato) al personal computer di ciascuno;
c. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Deve essere attivato su tutti i Personal Computer lo screen saver e la relativa password;
d. L'accesso ai dati presenti nel personal computer potrà avvenire quando si rende indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata

assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato;

e. È vietato installare autonomamente programmi informatici salvo autorizzazione esplicita dell'Amministratore di Sistema, in quanto sussiste il grave pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la struttura a gravi responsabilità civili ed 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.
f. È vietato modificare le caratteristiche impostate sul proprio PC, salvo con autorizzazione esplicita dell'Amministratore di Sistema;
g. È vietato inserire password locali alle risorse informatiche assegnate (come ad esempio password che non rendano accessibile il computer agli amministratori di rete), se non espressamente autorizzati e dovutamente comunicate all'Amministratore di Sistema;
h. È vietata l'installazione sul proprio PC di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pendrive, dischi esterni, i-pod, telefoni, ecc.), se non con l'autorizzazione espressa dell'Amministratore di Sistema. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

Art. 5 - Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (punto 22 del disciplinare tecnico). Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati sensibili e giudiziari (punto 21 del disciplinare tecnico) devono essere custoditi in archivi chiusi a chiave.

Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) obsoleti devono essere consegnati all'Amministratore di Sistema per l'opportuna distruzione.

Ogni qualvolta si procederà alla dismissione di un Personal Computer l'Amministratore di Sistema provvederà alla distruzione delle unità di memoria interne alla macchina stessa (hard-disk, memorie allo stato solido).

Art. 6 - Utilizzo di pc portatili

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, consiglio comunale, ecc…), in caso di allontanamento devono essere custoditi in un luogo protetto.

Art. 7 - Utilizzo delle stampanti e dei materiali di consumo

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come CD e DVD) è riservato esclusivamente ai compiti di natura strettamente istituzionale.

Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

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.

CAPO III - GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Art. 8 – Utilizzo della rete informatica

Le unità di rete sono aree di condivisione di informazioni strettamente professionali sulle quali vengono svolte regolari attività di controllo, amministrazione e backup e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato in queste unità, nemmeno per brevi periodi.

Si parte quindi dal presupposto che i files relativi alla produttività individuale vengono salvati sul server e i limiti di accesso sono regolarizzati da apposite policies di sicurezza che suddividono gli accessi tra gruppi e utenti.

L'amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza o in violazione del presente regolamento sia sui PC degli incaricati sia sulle unità di rete.

Le password d'ingresso alla rete ed ai programmi sono segrete e non vanno comunicate a terzi.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

E' importante togliere tutte le condivisioni dei dischi o di altri supporti configurate nel Personal Computer se non strettamente necessarie (e per breve tempo) allo scambio dei files con altri colleghi. Esse sono infatti un ottimo "aiuto" per i software che cercano di "minare" la sicurezza dell'intero sistema.

Sarà compito dell'Amministratore di Sistema provvedere alla creazione di un'area condivisa sul server per lo scambio dei dati tra i vari utenti.

Nell'utilizzo della rete informatica è fatto divieto di:

a. Utilizzare la Rete in modo difforme da quanto previsto dal presente regolamento;
b. Conseguire l'accesso non autorizzato a risorse di rete interne ed esterne alla Rete comunale;
c. Agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;

d. Effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc);
e. Installare componenti hardware non compatibili con l'attività istituzionale;
f. Rimuovere, danneggiare o asportare componenti hardware;
g. Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti;
h. Utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber o keylogger), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy;
i. Usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

Art. 9 - Utilizzo di Internet

l Personal Computer, qualora abilitati alla navigazione in Internet, costituiscono uno strumento necessario allo svolgimento della propria attività lavorativa.

Nell'uso di Internet e della Posta Elettronica non sono consentite le seguenti attività:

a. L'uso di Internet per motivi personali;
b. L'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc.);
c. Lo scaricamento (download) di software e di file non necessari all'attività istituzionale;
d. Utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Napster, Emule, Winmx, e-Donkey, ecc.);
e. Accedere a flussi in streaming audio/video da Internet per scopi non istituzionali (ad esempio ascoltare la radio o guardare video o filmati utilizzando le risorse Internet);
f. Un uso che possa in qualche modo recare qualsiasi danno all'Istituto o a terzi.

Art. 10 - Utilizzo della posta elettronica

La casella di posta, assegnata dall'Istituto, 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 della struttura per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali con l'istituto ricevuta da personale non autorizzato, deve essere visionata ed inoltrata al Capo Area, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto, non può essere comunicata all'esterno senza preventiva autorizzazione del Responsabile del trattamento.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

Per la trasmissione di file all'interno della struttura è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati (ad esempio per dimensioni superiori a 2 Mbyte è preferibile utilizzare le cartelle di rete condivise).

È obbligatorio controllare i file Attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web, HTTP o FTP non conosciuti) e accertarsi dell'identità del mittente.

Tutti coloro provvisti di indirizzo individuale, devono indicare il tutor del proprio account ossia la persona autorizzata ad aprire la posta del soggetto assente o quantomeno la persona che riceverà la posta del lavoratore assente.

Dopo tre mesi di assenza, l'account verrà disattivato e con esso la posta sarà trasferita ad un nuovo utente.

Per motivi di sicurezza la struttura non consente in alcun modo l'utilizzo di posta personale né attraverso l'uso di un webmail né utilizzando un client di posta.

In particolare nell'uso della Posta Elettronica non sono consentite le seguenti attività:

a. La trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali (D.lgs. 196 del 30/6/2003);
b. L'apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell'identità del mittente;
c. Inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici;
d. Inoltrare "catene" di posta elettronica (catene di S.Antonio e simili), anche se afferenti a presunti problemi di sicurezza.

CAPO IV. CONTROLLI e RESPONSABILITÀ

Art. 11 - Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del disciplinare tecnico allegato al D.lgs. n. 196/2003.

Art. 12- Amministrazione delle risorse informatiche

L'Amministratore di Sistema è il soggetto cui è conferito il compito di sovrintendere alle Risorse Informatiche dell'Istituto e a cui sono consentite in maniera esclusiva le seguenti attività:

a. Gestire l'hardware e il software di tutte le strutture tecniche informatiche di appartenenza dell'Istituto, collegate in rete o meno;
b. Gestire esecutivamente (creazione, attivazione, disattivazione e tutte le relative attività amministrative) gli account di rete e i relativi privilegi di accesso alle risorse, assegnati agli utenti della Rete Informatica comunale secondo quanto stabilito da ogni Capo Area;
c. Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi,

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;

d. Creare, modificare, rimuovere o utilizzare qualunque account o privilegio, 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. Rimuovere programmi software dalle risorse informatiche assegnate agli utenti, 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;
f. Rimuovere componenti hardware dalle risorse informatiche assegnate agli utenti, 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;
g. Utilizzare le credenziali di accesso di amministrazione del sistema, o l'account di un utente tramite reinizializzazione della relativa password, per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di prolungata assenza, irrintracciabilità o impedimento dello stesso. Tale utilizzo deve essere esplicitamente richiesto dal Capo Area dell'utente assente o impedito e deve essere limitato al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

Art. 13 - Non osservanza del regolamento

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con i provvedimenti disciplinari e le azioni, civili e penali, consentite.

La contravvenzione alle regole contenute nel presente regolamento da parte di un utente, comporta l'immediata revoca delle autorizzazioni ad accedere alla Rete Informatica ed ai servizi/programmi autorizzati, fatte salve le sanzioni più gravi previste dalle norme vigenti.

Se i lavoratori perseverassero nell'uso ed abuso degli strumenti elettronici a loro disposizione, il datore è autorizzato a procedere per step, con controlli prima sul reparto, poi sull'ufficio ed, infine, sul gruppo di lavoro; solo a questo punto, ripetendosi l'anomalia, sarà lecito il controllo su base individuale.

Art. 14 - Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento.

Le proposte verranno esaminate dal Consulente dell'Ente.

Il presente Regolamento è altresì soggetto a revisione periodica, secondo necessità, in base alle disposizioni legislative e ministeriali via via emanate.

Approvato

dal Consiglio d'Istituto del 26 Maggio 2011

ALLEGATO: GLOSSARIO DEI TERMINI TECNICI E INFORMATICI

Account	Iscrizione registrata su un server e che, tramite l'inserimento di una userld e di una password, consente l'accesso alla rete e/o ai servizi. Ad esempio, un account ci permette di entrare in Internet, un altro account ci serve per ricevere e spedire posta elettronica. Un account ci consente di accedere alle risorse di una rete locale, come server, file server, stampanti. Altri account servono per accedere a server e servizi vari.
Antivirus	Tipo di software che cerca e distrugge gli eventuali programmi virus e cerca di rimediare ai danni che hanno compiuto.
Backup	Copia di riserva di disco, di una parte del disco o di uno o più file.
Database	(Base di Dati). Qualsiasi aggregato di dati organizzato in campo (colonne) e record (righe).
Download	Registrare sul proprio disco rigido un file richiamandolo, tramite modem o rete, da un computer, da un server o da un host (tramite Internet, rete locale o geografica).
E-mail	Electronic mail, posta elettronica. Scambio di messaggi e di file attraverso una rete locale o Internet. Avviene in tempo reale ed è indipendente dalla posizione fisica dei computer mittente e destinatario. I messaggi e file vengono conservati da un server che provvede ad inoltrarli al destinatario quando questo si collega.
Firewall	Insieme di software/hardware usato per filtrare i dati in scambio fra reti diverse, al fine di proteggere un server da attacchi pervenuti via rete locale o via Internet. Consente il passaggio solamente di determinati tipi di dati, da determinati terminali e determinati utenti.
Freeware	Software gratuito realizzato e distribuito da privati o piccole società, attraverso Internet o CD-ROM allegati a pubblicazioni in edicola.
Hardware	Letteralmente ferramenta, in informatica si intende l'insieme dei componenti (CPU, Hard Disk ecc.) che costituiscono un computer.
Internet	La madre di tutte le reti di computer. E' l'insieme mondiale delle reti di computer interconnesse.
Intranet	Rete locale che, pur non essendo necessariamente accessibile dall'esterno, fa uso di tecnologie Internet.
MP3 (MPEG-4)	Tecnologia per la compressione/decompressione di file audio che consente di mantenere una perfetta fedeltà e qualità anche riducendo il file audio di ben 11 volte la lunghezza originale.
MPG (Motion Picture Experts Group)	Stabilisce gli standard digitali per audio e video.
Password	Parola che consente l'accesso di un utente ad una rete, ad un servizio telematico o ad un sito Internet. E' necessario digitarla esattamente, assieme alla user-id.
Quicktime	Standard definito dalla Apple e utilizzato da tutti i computer per la riproduzione fedele dei filmati video.
Software	Sono i programmi (professionali, ludici, video, musicali, raccolte di suoi ed immagini) per i computer.
Streaming	Con il termine **streaming** si intende un flusso di dati audio/video trasmessi da una sorgente a una o più destinazioni su Internet.
Url filtering	Sistema che permette di monitorare e filtrare la navigazione in Internet, bloccando l'accesso a particolari categorie di siti, al fine di limitare il rischio di utilizzo improprio della rete e la navigazione in siti non pertinenti o non compatibili con l'attività aziendale.
User Id	Nome utente
Utente (User)	Chiunque utilizzi un elaboratore collegato alla rete, sia che il collegamento avvenga in rete locale sia che si tratti di un accesso remoto.
Virus	Un programma creato per diffondersi da computer a computer, spesso danneggiando i dati e gli altri programmi registrati.