**DIREZIONE DIDATTICA II CIRCOLO**
**Via G. Iervolino, 335 – 80040 POGGIOMARINO**
Tel./ Fax 0818651167 – E-mail: naee15800g@istruzione.it
P.E.C.: naee15800g@pec.istruzione.it
C.F. 82008130633 – Codice Univoco dell'Ufficio UFMVJL

# Regolamento per l'utilizzo dell'infrastruttura informatica dell'Istituto Scolastico

# (POLICY della Scuola)

Approvato con deliberazione n.24 del Consiglio di Istituto del _29/10/2019.

## Regolamento per l'utilizzo dell'infrastruttura informatica dell'Istituto Scolastico

L'istituzione scolastica indicata in intestazione del presente documento (in prosieguo denominata Istituto),

VISTO il D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali", sostituito con il Regolamento Europeo 679/2016 più noto come GDPR;
VISTO il Regolamento emanato dal Ministero della Pubblica Istruzione con decreto 7 dicembre 2006 n. 305;
VISTO il provvedimento del Garante del 1° marzo 2007, per l'utilizzo della posta elettronica e l'accesso alla rete internet;
VISTE la Legge 7 agosto 1990 n. 241 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" e la Legge 11 febbraio 2005 "Modifiche ed integrazioni alla legge 7/8/90 n. 241 concernenti norme generali sull'azione amministrativa";
VISTO il DPR del 28/12/2000 n. 445 "Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";
VISTO il D. Lgs. 7 marzo 2005 n. 82 "Codice dell'Amministrazione Digitale" e ss.mm.ii;
CONSIDERATO che l'Istituto tra i vari strumenti di lavoro ha messo a disposizione dei dipendenti accessi ad internet e servizi di caselle di posta elettronica per lo svolgimento delle mansioni e compiti loro affidati;
RICHIAMATO il principio generale che l'utilizzo delle risorse ICT che la scuola mette a disposizione dei dipendenti deve sempre ispirarsi a criteri di diligenza e correttezza normalmente adottati nell'ambito dei rapporti di lavoro;
RILEVATO che l'Autorità Garante per la Privacy, con delibera n. 13 del 1.3.2007 (pubblicata in G.U. del 10.3.2007 n. 58) ha inteso precisare che è opportuno da parte dei Datori di Lavoro adottare un disciplinare interno redatto in modo chiaro, senza formule generiche ed adeguatamente pubblicizzato verso i singoli dipendenti interessati, anche ai fini dell'esercizio del potere disciplinare;
RITENUTO che l'adozione del regolamento consente di escludere l'applicabilità della normativa penale a tutela della corrispondenza elettronica poiché, essendo considerata strumento di lavoro, non può essere considerata corrispondenza privata;
CONSIDERATO, inoltre, che, se correttamente applicato e fatto rispettare, il regolamento può risultare un efficace strumento della Policy scolastica anche al fine di limitare il rischio di insorgenza di responsabilità amministrativa dell'Istituto;
RITENUTO, pertanto, di dover adottare apposito regolamento per l'utilizzo infrastruttura informatica dell'Istituto nonché di Internet e della Posta Elettronica in cui è, tra l'altro, precisato che gli stessi sono strumenti aziendali e come tali soggetti anche a controlli secondo i principi ed i criteri di cui ai commi 5, 6 e 7 del citato Provvedimento del Garante e della normativa in tema di Protezione dei dati personali D. Lgs.196/2003 n. 196 e del D.M. 35 del 7 dicembre 2006;
TENUTO CONTO che il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, a tutti i collaboratori della scuola, interni od esterni, ai collaboratori a progetto ed a quelli che durante il periodo di stage, a prescindere dal rapporto contrattuale con la stessa intrattenuto, nonché agli alunni;
CONSIDERATA la necessità di contemperare l'obbligo di adozione di misure di protezione dei dati trattati con strumenti informatici e di prevenzione dei rischi che incombono sugli stessi a seguito del relativo utilizzo, con l'esigenza di tutelare la dignità dei lavoratori e il diritto alla riservatezza dei loro dati personali,

**ADOTTA**

il presente regolamento allegato al presente atto che né forma parte integrante e sostanziale, al fine di descrivere le caratteristiche e le regole di utilizzo della rete interna e l'accesso alla rete internet e della posta elettronica e di informare gli utilizzatori (dipendenti, docenti, studenti, genitori) sui controlli effettuati e sul trattamento eseguito sui loro dati personali, in conseguenza delle misure adottate per la protezione degli strumenti informatici.

Il regolamento sarà aggiornato ,se necessario, in occasione della revisione periodica del documento programmatico sulla sicurezza, o in caso di rinvenimento di soluzioni tecnologiche ritenute più idonee a tutelare i dati personali o in caso di variazione della normativa vigente. Il regolamento sarà pubblicato sul sito internet, nella sezione Privacy, oltre che nella bacheca d'istituto e all'albo pretorio, così da portarlo a conoscenza di tutti.

La DIRIGENTE SCOLASTICA
Titolare del Trattamento dei dati
***Dott.ssa Cristina IERVOLINO***

**Indice**

## Regolamento per l'utilizzo dell'infrastruttura informatica dell'Istituto Scolastico

### PREMESSA

Negli anni l'uso delle tecnologie informatiche nella didattica e nella gestione generale della scuola è aumentato vertiginosamente, tanto che oggi è impossibile fare didattica e lavorare senza l'accesso alla rete, sia locale che esterna. Internet è molto utile, però può essere anche una potenziale fonte di rischi, tanto maggiore quanto meno si conoscono i modi legittimi di utilizzo e si abbia scarsa consapevolezza delle funzioni della rete. Questo vale certamente per il complesso sistema di computer in rete presenti nella scuola: sia riguardo ai tradizionali laboratori, sia riguardo agli uffici amministrativi e più in generale alle aule singole predisposte per il collegamento interno ed esterno. Le norme che seguiranno richiamano gli utenti ad un uso corretto e generalizzato delle infrastrutture di rete (interna ed esterna), il cui uso improprio può generare problemi, da un punto di vista didattico; nonché difficoltà di uso delle macchine, con possibili danni al loro funzionamento e connessi danni di natura economica. Le **responsabilità civili e penali** potenzialmente derivanti dall'uso improprio delle TIC (Tecnologie dell'Informazione e della Comunicazione) sono note. E' dunque importante definire, all'interno dell'Istituto, alcune regole chiare che permettano di lavorare in modo sereno e consentano di usare le tecnologie in modo efficiente e positivo. Queste indicazioni vogliono favorire anche un uso consapevole e critico delle tecnologie informatiche, con la dovuta competenza, a seconda dei diversi gradi di utilizzo.

Questo documento costituisce parte integrante del Regolamento di Istituto per la gestione dei dati personali ai sensi del vigente regolamento europeo 679/2016 e si adatta ai reali utilizzi quotidiani delle TIC. Verrà portato a conoscenza di tutti gli utenti: studenti/genitori personale della scuola tramite la pubblicazione sul sito internet dell'Istituto e sarà revisionato annualmente. Il presente regolamento, da un punto di vista legislativo e amministrativo, è ispirato e promosso da direttive del Ministero dell'Istruzione a livello nazionale e regionale e fa costante riferimento alle norme legislative specifiche del settore.

### ART. 1 OGGETTO E AMBITO DI APPLICAZIONE

Il presente regolamento disciplina le modalità di accesso, di uso della rete informatica e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire all'interno e all'esterno dell'Istituzione scolastica.
La rete dell'Istituzione scolastica 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 della scuola. Il patrimonio informativo è l'insieme delle banche dati in formato digitale ed 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 della scuola. Per utenti interni si intendono tutti gli amministrativi, i docenti e i collaboratori scolastici. Per utenti esterni si intendono le ditte fornitrici di *software* che effettuano 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 e i collaboratori esterni, attività di stage, relatori e formatori per corsi di aggiornamento.

## ART. 2 PRINCIPI GENERALI – DIRITTI E RESPONSABILITÀ

L'Istituto promuove l'utilizzo della rete informatica, di internet e della posta elettronica quali strumenti utili a perseguire le proprie finalità istituzionali.
Ogni utente è responsabile **civilmente** e **penalmente** del non corretto uso delle risorse informatiche, dei servizi/programmi ai quali ha accesso e dei propri dati.
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 del regolamento Europeo 679/2016, più noto come GDPR e la normativa collegata.
E' vietato:

1. utilizzare giochi (né in locale, né in rete esterna);
2. inviare a nessuno fotografie/video di alunni, nè di personale della scuola (Dirigente, Docenti, Collaboratori, Amministrativi, Esperti Esterni);
3. fotografare documenti non destinati alla diffusione;
4. fotografare documenti privati;
5. registrare e diffondere audio vocali o filmati all'insaputa dell'interessato;
6. Effettuare manutenzione degli apparati se non esplicitamente autorizzati e con idonne capacità tecniche, al fine di evitare danni ai componenti;
7. Download non autorizzato di programmi/applicazioni che possono diffondere virus o alterare la stabilità degli altri elaboratori danneggiandoli e/o mettendo a rischio l'integrità dei dati e quindi la riservatezza;
8. Download di dati non autorizzati (musica, giochi, video, vedere video in streaming, …)
9. Installare software privo della regolare licenza d'uso;
10. Qualsiasi applicazione per effettuare chatt e ogni tipo di social network se non esplicitamente autorizzato;
11. Installare e collegare strumenti informatici alla rete locale dell'Istituto se non sono state verificate le misure di sicurezza;
12. Navigare nella rete locale interna dell'istituto aprendo cartelle e file non autorizzate;
13. E' vietato ogni altro utilizzo non esplicitamente consentito dal Titolare o dal Responsabile del Trattamento dei dati, o dall'Amministratore di Sistema;

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 all'Amministratore di Sistema, a garanzia e tutela delle informazioni di carattere personale dei lavoratori.
L'Amministratore di Sistema cura l'attuazione del presente regolamento attraverso la predisposizione di Procedure Operative che verranno diffuse tra tutti i dipendenti.

Tali procedure nonché il presente regolamento devono essere rese facilmente e continuativamente disponibili per consultazione sui normali mezzi di comunicazione all'interno della struttura (es. sito internet, intranet, bacheche, newsletter….)

## ART. 3 UTILIZZO DEI PERSONAL COMPUTER

Il *personal computer* affidato al dipendente **è uno strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza e pertanto è **vietato**.

In particolare:

L'accesso all'elaboratore deve essere protetto da *password* che viene custodita dal Titolare del trattamento dati e non divulgata. La *password* deve essere attivata per l'accesso alla rete, per lo *screensaver* e per il *software* **Non è consentita** l'attivazione della *password* di accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.
Laddove sia possibile, la *password* di accesso al sistema deve essere gestita mediante un sistema elettronico centralizzato, che permetta la gestione crittografata e la possibilità della modifica da parte dell'Amministratore di Sistema nel caso fosse necessario. Una gestione centralizzata, quindi mediante dominio informatico, permette anche di applicare delle *policy di sicurezza delle password* quali la complessità, la durata, il riuso, etc in maniera centralizzata, semplificando le attività di gestione/manutenzione degli account.
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 o in caso di assenza autorizzato dal Titolare o dal Responsabile al trattamento dei dati) al *personal computer* di ciascuno incaricato;
Il *PC* deve essere spento ogni sera, o al termine delle lezioni o del servizio, prima di lasciare gli uffici o i laboratori di informatica, 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 *PC* lo *screensaver* e richiedere la relativa *password* dopo un tempo non superiore a 15 minuti di inattività.
Ai fini di un corretto risparmio energetico, impostare anche l'oscuramente del monitor dopo 5 minuti di inutilizzo, e la sospensione dell'elaboratore dopo 30 minuti di inattività. Analoga attività deve essere espletata anche sulle stampanti di piano, così da limitare il consumo energetico.
L'account utente non deve avere privilegi amministrativi, al fine di evitare, anche involontariamente, la modifica della configurazione del sistema, l'installazione di programmi o agenti malevoli.
È vietato installare autonomamente programmi informatici sui *server* salvo autorizzazione esplicita dell'Amministratore di Sistema, e sui *PC* salvo autorizzazione del Titolare, in quanto sussiste il grave pericolo di diffondere *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.

Su ogni computer e server deve essere installato un *software antivirus* e le firme per identificare nuovi virus devono essere aggiornate ogni giorno. L'esperienza pratica insegna che l'uso di software antivirus free comunemente scaricabile da internet non ha gli stessi risultati di analoghi prodotti distribuita da case produttrici di livello internazionale specializzati nella protezione degli strumenti informatici. Sarà cura dell'Amministratore di Sistema mantenere aggiornate le firme degli anti-virus e le relative licenze d'uso, acquistandole/rinnovandole prima della scadenza previa comunicazione/autorizzazione con il Responsabile del Trattamento dei dati o Titolare.

nel caso il software antivirus rilevi la presenza di un virus, sospendere immediatamente ogni elaborazione in corso, senza spegnere il PC e segnalare prontamente l'accaduto al Amministratore di Sistema.

È vietato modificare le caratteristiche impostate sul proprio *PC*, salvo autorizzazione esplicita dell'Amministratore di Sistema o del Responsabile al Trattamento dei dati o del Titolare.

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.

È vietata l'installazione sul proprio *PC* di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, *modem*, dischi esterni, *i-pod*, telefoni, ecc.), se non con l'autorizzazione espressa dell'Amministratore di Sistema o del Dirigente Scolastico.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema o il Responsabile al trattamento dei dati o il Titolare, nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

In caso di prolungata assenza e in ogni caso fosse necessario accedere ad una postazione di lavoro assegnata ad un dipendente, il Titolare o Responsabile del Trattamento dei dati può autorizzare l'Amministratore di Sistema alla modifica della password di accesso.

La password di accesso al computer deve rispettare le seguenti caratteristiche:

14. *Lunghezza minima*: 8 caratteri
15. *Complessità*: utilizzo di caratteri speciali, almeno una maiuscola, almeno un numero
16. *Durata*: la password deve avere una scadenza non più lunga di 90 giorni
17. *Riuso*: Non è possibile utilizzare le ultime 3 password già utilizzate

## ART. 4 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.**

**I *file* contenenti informazioni inerenti l'attività lavorativa devono obbligatoriamente essere salvati sul *server*** e i limiti di accesso a tali risorse devono essere regolarizzati da apposite procedure di sicurezza che suddividono gli accessi tra gruppi e utenti.

Le cartelle condivise a gruppi di utenti dovranno contenere solo i file da condividere con più utenti.

Le cartelle accessibili al singolo utente devono contenere i file utilizzati dal singolo utente. L'organizzazione interna alla cartella può essere creta mediante la suddivisione in directory (più note come cartelle) così da organizzare logicamente la memorizzazione dei file, facilitandone la ricerca.

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, dandone comunicazione al dipendente ed al Responsabile del Trattamento dei dati ed al Titolare.

Sulle unità di rete vengono svolte regolari attività di controllo essendo esse il patrimonio informativo dell'Istituto, provvedendo ai relativi salvataggi;

Le *password* d'ingresso alla rete ed ai programmi sono segrete e non vanno comunicate a terzi, tranne (in situazioni di urgenza) quando si rende indispensabile ed indifferibile l'intervento per esclusive necessità di funzionalità operativa degli uffici e di sicurezza del sistema.

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, evitando sia lo spreco di risorse che la perdita di informazioni per errato aggiornamento dei file.

È compito dell'Amministratore di Sistema provvedere alla creazione e alla manutenzione di aree condivise sul *server* per lo scambio dei dati tra i vari utenti. Potrà suggerire lo spostamento/cancellazione dei dati da tali risorse condivise e spostarle nelle cartelle dell'utente che segue lo specifico procedimento.

L'Amministratore di Sistema dovrà configurare lo scanner di rete in modo da memorizzare le scansioni nelle cartelle dei singoli utenti.

Nell'utilizzo della rete informatica è fatto **divieto** di:

1. utilizzare la Rete in modo difforme da quanto previsto dal presente regolamento.
2. agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
3. effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc);
4. installare/rimuovere/danneggiare componenti hardware non compatibili con l'attività istituzionale;
5. modificare i collegamenti della strumentazione o effettuarne di nuovi senza il consenso dei responsabili del laboratorio e/o dell'Amministratore del Sistema;
6. utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare file e software di altri utenti;
7. 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;
8. usare l'anonimato o servirsi di risorse che consentano di restare anonimi;

## ART. 5 UTILIZZO DI INTERNET

La rete internet rappresenta una risorsa strategica per l'Istituto ai fini lavorativi e formativi. E' un bene comune e con performance bilanciate in base al carico di utilizzo ed ai costi di connettività, pertanto il relativo uso deve essere fatto solo per scopi istituzionali.

I *PC* abilitati alla navigazione in *Internet* costituiscono uno strumento necessario allo svolgimento dell'attività lavorativa.

La rete internet rappresenta un veicolo di diffusione di programmi malevoli, pertanto è necessario **utilizzare un firewall** che permetta di proteggere accessi non consentiti dall'esterno, ma anche di poter applicare delle policy per limitare/evitare un abuso dell'utilizzo della rete, tramite dei *content filtering* che bloccano/consentono l'accesso a pagine web o all'esecuzione di applicazione che necessitano della rete internet. L'Istituto, in ogni caso, non può farsi carico delle responsabilità per il materiale non idoneo trovato o per eventuali conseguenze causate dall'accesso al Web. Per tale ragione, gli utilizzatori devono essere pienamente coscienti dei rischi a cui si espongono collegandosi alla rete, riconoscendo ed evitando gli aspetti negativi (pornografia, violenza, razzismo …).

Separare la rete degli uffici amministrativi dalla rete della didattica e dalla rete WiFi.

Nell'uso di internet e della posta elettronica **non** sono **consentite** le seguenti attività:

1. l'uso di internet per motivi personali;
2. l'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, social network, ecc.);
3. lo scaricamento (download) o l'inserimento (upload) di software e di file non necessari all'attività istituzionale;
4. utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Napster, Emule, Winmx, e-Donkey, ecc.);
5. accedere a flussi in streaming audio/video da internet per scopi non istituzionali;
6. un uso che possa in qualche modo recare qualsiasi danno all'Istituto o a terzi.

Si suggerisce di associare ad ogni utente

7. una quota massima giornaliera/settimanale/mensile di download-upload così da poter monitorare il relativo utilizzo in maniera macro-aggregata, senza analizzare i siti visitati;
8. una back-list di siti non visitabili, casomai utilizzando degli appostiti filtri dei contenuti;
9. Di creare diversi livelli di accesso, in base all'autenticazione preventiva per l'accesso ad internet oppure mediante indirizzo IP della postazione di lavoro, individuando le seguenti le seguenti 3 categorie:
   a) Dirigente e Responsabile al trattamento dei dati
   b) Collaboratori Scolastici
   c) Laboratorio didattico e Wifi

| Categoria filtro web | Dirigente | Segreteria | Laboratori |
|---|---|---|---|
| Security Threat | | | |
| Anonymizers | negare | negare | negare |

| | | | |
|---|---|---|---|
| Malware | negare | negare | negare |
| Phishing & Fraud | negare | negare | negare |
| Botnets | negare | negare | negare |
| Network Errors | negare | negare | negare |
| Spam Sites | negare | negare | negare |
| Compromised | negare | negare | negare |
| Parked Domains | negare | negare | negare |
| Managed Categories | | | |
| Advertisements & Pop-Ups | consenti | consenti | negare |
| Business | consenti | consenti | negare |
| Forums & Newsgroups | consenti | consenti | negare |
| Dating & Personals | consenti | consenti | negare |
| Entertainment | consenti | negare | negare |
| Games | consenti | negare | negare |
| Health & Medicine | consenti | negare | negare |
| Streaming Media & Downloads | consenti | negare | solo youtube |
| Nudity | negare | negare | negare |
| Pornography/Senegareually Enegareplicit | negare | negare | negare |
| Restaurants & Dining | consenti | negare | negare |
| Social Networking | consenti | negare | negare |
| Travel | consenti | negare | negare |
| Web-based Email | consenti | consenti | negare |
| Cults | consenti | consenti | negare |
| Hacking | negare | negare | negare |
| Information Security | consenti | consenti | negare |
| Private IP Addresses | consenti | consenti | negare |
| Tasteless | consenti | consenti | negare |
| Alcohol/Tobacco | consenti | negare | negare |
| Transportation | consenti | consenti | negare |
| Computers & Technology | consenti | consenti | negare |
| Download Sites | consenti | consenti | negare |
| Finance | consenti | consenti | negare |
| Government | consenti | consenti | negare |
| Illegal Drugs | consenti | negare | negare |
| News | consenti | consenti | negare |
| Personal Sites | consenti | consenti | consenti |
| Real Estate | consenti | consenti | negare |
| Search Engines/Portals | consenti | consenti | negare |
| Sports | consenti | negare | negare |
| Violence | consenti | negare | negare |
| General | consenti | consenti | consenti |
| Fashion & Beauty | consenti | negare | negare |
| Illegal Software | consenti | negare | negare |
| Instant Messaging | consenti | negare | negare |
| School Cheating | consenti | negare | negare |
| Child Abuse Images | consenti | negare | negare |
| Arts | consenti | consenti | consenti |

| | | | |
|---|---|---|---|
| Chat | consenti | negare | negare |
| Criminal Activity | consenti | negare | negare |
| Education | consenti | consenti | consenti |
| Gambling | consenti | negare | negare |
| Hate & Intolerance | consenti | consenti | negare |
| Job Search | consenti | consenti | negare |
| Non-profits & NGOs | consenti | consenti | negare |
| Politics | consenti | consenti | negare |
| Religion | consenti | consenti | negare |
| Shopping | consenti | negare | negare |
| Translators | consenti | consenti | consenti |
| Weapons | consenti | negare | negare |
| Leisure & Recreation | consenti | consenti | negare |
| Greeting Cards | consenti | negare | negare |
| Image Sharing | consenti | negare | negare |
| Peer to Peer | negare | negare | negare |
| Senegare Education | negare | negare | negare |

Per le applicazioni, invece, le regola da applicare sono:

| Categoria applicazioni consentite | Dirigente | Segreteria | Laboratorio |
|---|---|---|---|
| Business | forward | forward | drop |
| Bypass_Proxies_and_Tunnels | forward | forward | drop |
| Database | forward | forward | forward |
| File_Transfer | forward | forward | forward |
| Games | forward | drop | drop |
| Instant_messaging | forward | drop | drop |
| Mail_and_Collaboration | forward | forward | forward |
| Mobile | forward | forward | forward |
| Network_Management | forward | forward | forward |
| Network_Protocols | forward | forward | forward |
| P2P | drop | drop | drop |
| Private_Protocol | forward | forward | forward |
| Remote_Access_Terminals | forward | forward | drop |
| Security_Update | forward | forward | forward |
| Social_Network | forward | drop | drop |
| Streaming_Media | forward | forward | forward |
| Voice_over_IP | forward | forward | forward |
| Web | forward | forward | forward |
| Web_IM | forward | drop | drop |

## ART. 6 UTILIZZO DELLA POSTA ELETTRONICA

La casella di posta elettronica è utilizzata per le comunicazioni ufficiali: convocazioni riunioni, comunicazioni di servizio anche dirette al singolo dipendente, ordine di servizio, materiale preparatorio alle riunioni collegiali, circolari, copia elettronica di documenti redatti su supporti cartacei, disposizioni

sulla sicurezza informatica, ..., pertanto è necessario controllare frequentemente il contenuto della mail. Le comunicazioni devono avvenire solo tramite la mail istituzionale dell'Istituto.

Ogni utente è responsabile del corretto utilizzo della stessa ed è tenuto a:

1. conservare la password nella massima riservatezza e con la massima diligenza,
2. mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti,
3. utilizzare l'account per l'invio di comunicazioni attinenti all'attività lavorativa,
4. inviare preferibilmente file in formato PDF,

Agli utenti è fatto divieto di qualsiasi uso della posta elettronica che possa in qualche modo recare danno all'istituto o a terzi e quindi di:

1. prendere visione della posta altrui,
2. simulare l'identità di un altro utente, ovvero utilizzare per l'invio di messaggi credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza,
3. utilizzare strumenti software o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'istituto, trasmettere a mezzo posta elettronica dati sensibili, personali o commerciali di alcun genere,
4. se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati,
5. utilizzare il servizio di posta elettronica per inoltrare giochi, scherzi, barzellette, appelli e
6. petizioni, messaggi tipo "catene" e altre e-mails che non siano di lavoro.

È fatto divieto di utilizzare le caselle di posta elettronica della struttura per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione, che esulino dagli scopi della scuola.

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.

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 o del Titolare.

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 5 MB è preferibile utilizzare le cartelle di rete condivise).

È obbligatorio controllare i file attachments (ALLEGATI) 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.

In particolare nell'uso della posta elettronica non sono consentite le seguenti attività:

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 e inerenti le ragioni di servizio. In tale ultimo caso è necessario utilizzare la crittografia per proteggere le informazioni trasferite con una chiave di decifratura trasmessa al destinatario mediante un diverso canale (es. tramite SMS);

l'apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell'identità del mittente;

inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici.

Modificare la password della posta elettronica almeno ogni 6 mesi;

## ART. 6 UTILIZZO DELLE *PASSWORD*

Le password di ingresso alla rete, di accesso ai programmi e dello screensaver, sono previste ed attribuite dall'Incaricato della custodia delle Password, ovvero dal Titolare. Se le password di accesso alla rete sono gestite tramite un dominio informatico allora non è necessario la gestione cartacea.

È necessario procedere alla modifica della password a cura dell'Amministratore di Sistema o dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni tre mesi con contestuale comunicazione all'Incaricato della custodia delle Password in busta chiusa, qualora previsto.

La comunicazione di variazione delle password dovrà essere consegnata al Titolare in busta chiusa, con data e firma dell'incaricato apposte sul lembo di chiusura.

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato (punto 5 del disciplinare tecnico).

La password deve essere immediatamente sostituita, dandone comunicazione scritta all'Incaricato della custodia delle password, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia, per iscritto, al Titolare.

## ART. 7 UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (hard drive esterni, chiavi USB, CD riscrivibili) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati sensibili e giudiziari devono essere custoditi in archivi chiusi a chiave.

Tutti i supporti magnetici riutilizzabili (hard drive esterni, 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 o all'archiviazione protetta delle unità di memoria interne alla macchina stessa (hard-disk, memorie allo stato solido).

## ART. 8 UTILIZZO DI *PC* PORTATILI *TABLET O ALTRO DEVICE*

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, lavoro domestico autorizzato, ecc…), in caso di allontanamento devono essere custoditi in un luogo protetto.

## ART. 9 UTILIZZO DELLE STAMPANTI E DEI MATERIALI DI CONSUMO

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, 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. In caso di necessità la stampa in corso può essere cancellata.

L'uso di stampanti centralizzate deve prevedere la stampa con il pin: l'incaricato che stampa un documento, per evitare che il file stampata possa mischiarsi con altre stampe in coda, deve digitare un proprio pin, così che la stampa sarà effettuata solo in quel momento e quindi ritirata dalla stampante centralizzata. E' opportuno che ogni utente abbia un proprio pin in modo da poter monitorare l'uso della stampante centralizzata sia per la stampa che per le copie

La stampante centralizzata se dotata anche di scanner può essere configurata in modo che ogni utente possa digitalizzare i documenti cartacei ed il relativo file generato venga salvato nella propria cartella di rete o in quella condivisa al gruppo. E' buona norma programmare la stampante in modo da generare un file non di grandi dimensioni, così da poter inviare anche mediante posta elettronica.

## ART. 10 REATI E VIOLAZIONI DI LEGGE

Al di là delle regole di buon senso ed educazione, vi sono comportamenti, talvolta solo apparentemente innocui, che possono portare gli autori a commettere veri e propri reati e, di conseguenza, a subire procedimenti penali. Quelli di seguito sono alcuni esempi di reati informatici (o che comunque possono essere posti in essere col mezzo informatico):

1. Accesso abusivo ad un sistema informatico e telematico
2. Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico
3. Danneggiamento informatico
4. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

5. Frode informatica
6. Ingiuria
7. Diffamazione
8. Minacce e molestie.

L'Istituto, al fine di prevenire condotte inappropriate degli utenti, potenzialmente riconducibili ai reati di cui sopra, ha fissato le norme definite in questo regolamento da rispettare e far rispettare rigorosamente e ha indicato i comportamenti corretti da tenere.

**ART. 11 AMMINISTRATORE DI SISTEMA**

L'Amministratore di Sistema è il soggetto cui è conferito da parte del Titolare il compito di sovrintendere alle risorse informatiche dell'Istituto e a cui sono consentite in maniera esclusiva le seguenti attività:

1. gestire l'hardware e il software di tutte le strutture tecniche informatiche di appartenenza dell'Istituto, collegate in rete o meno, e aggiornare l'inventario con cadenza almeno semestrale;
2. 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 istituzionale, secondo le direttive impartite dal Titolare;
3. 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;
4. creare, modificare, rimuovere o utilizzare qualunque account o privilegio con l'autorizzazione del Titolare, 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;
5. 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;
6. 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;
7. utilizzare le credenziali di accesso di amministrazione del sistema, o l'account di un utente tramite re inizializzazione 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 Titolare per l'utente assente o impedito, e deve essere limitato al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.
8. promuove all'interno dell'Istituto l'uso del software non proprietario (opensource) come da indicazioni ministeriali.

## Art. 15 UTILIZZO LABORATORI DI INFORMATICA COMPUTER PORTATILI E LIM

Il laboratorio di informatica è un'aula chiusa a chiave il cui accesso deve essere prenotato casomai già all'interno dell'orario di classe, così da evitare accavallamenti di classi e sapere sempre chi lo abbia utilizzato.

Durante le attività è Responsabile della strumentazione il singolo docente che dovrà segnalare al Titolare / Responsabile del trattamento dei dati ogni tipo di abuso, danno o mal utilizzo così da prontamente individuare gli autori ed adottare le dovute sanzioni;

I computer portatili sono in consegna presso il laboratorio di informatica. I docenti che ne abbiano esigenze di utilizzo ne fanno esplicita richiesta. I portatili sono già configurati per l'accesso alla rete WiFi.. A termine dell'utilizzo dovranno essere riposti nel laboratorio di informatica. I docenti utilizzatori rispondono di ogni malevole utilizzo, danno o furto degli stessi.

Quasi tutte le aule sono dotate di LIM e computer portatile. I docenti utilizzatori rispondono di ogni malevole utilizzo, danno o furto degli stessi.

## ART. 12 SITO WEB DELLA SCUOLA E SERVIZI ON-LINE ALLE FAMIGLIE, STUDENTI, DOCENTI/UTENTI ESTERNI

Sarà cura dell'Amministratore di Sistema o qualora individuato il Referente per la gestione del sito (da non confondere con webmaster che si occupa in generale della manutenzione ed aggiornamento del contenitore WEB) per la pubblicazione delle informazioni sul sito internet della scuola, nonché la garanzia che il contenuto sul sito sia tempestivamente aggiornato.

La richiesta di pubblicazione delle informazioni deve avvenire esclusivamente tramite posta elettronica, trasmettendo il testo, gli allegati ed il periodo di inizio e fine pubblicazione. L'Amministratore non è responsabile del contenuto pubblicato. La responsabilità è di colui che richiede la pubblicazione, avendo chiesto ed ottenuto il permesso alla pubblicazione qualora il documento da pubblicare contenga informazioni riservate (diritto d'autore) e/o il consenso alla pubblicazione se sono oggetto a dati personali (es. foto).

La scuola non pubblicherà materiale prodotto dagli alunni senza il permesso dei loro genitori; inoltre, le fotografie degli stessi saranno pubblicate solo se è stato acquisito il consenso dei loro genitori. Le fotografie degli studenti sul sito della scuola saranno selezionate in modo tale che solo gruppi di alunni siano ritratti in attività didattiche a scopi documentativi.

La scuola offre all'interno del proprio sito web i seguenti servizi alle famiglie ed agli utenti esterni: consultazione elenchi libri di testo; piano dell'offerta formativa; regolamento di istituto; informazioni generali sull'istituto; informazioni sui progetti attivati dall'istituto; informazioni sull'amministrazione dell'istituto; albo di istituto; avvisi e comunicazioni; moduli vari; sezione area riservata; circolari per i docenti; ed altro.

Nel sito della scuola può essere consultato dai soggetti abilitati anche il registro elettronico: strumento on-line facente le funzioni di registro di classe e registro personale del docente con accesso con credenziali da parte dei genitori per valutazioni, note, programmi svolti.

L'Istituto si impegna a mantenere efficienti questi servizi, a migliorarli e estenderli nell'ottica di aumentare la qualità del servizio offerto.

**ART. 13 WI-FI**

L'Istituto è dotato di diversi hotspot per la connessione Wi-fi e quindi collegarsi ad internet.

L'Amministratore di sistema, in attesa di una radicale re-ingegnerizzazione del sistema di registrazione alla rete scolastica, configura i *device* che possono accedere alla Wi-Fi, registrando nell'apposita lista il MAC address autorizzati dal Dirigente Scolastico esclusivamente al personale docente e non docente.

Periodicamente tale lista viene aggiornata. Non appena sarà attivato uno strumento centralizzato per la gestione dei log verrà aggiornato tale articolo.

**ART. 14 UTILIZZO DI TELEFONINI E ALTRE APPARECCHIATURE DI REGISTRAZIONE DI IMMAGINI E SUONI**

Il telefono personale deve essere utilizzato solo per chiamate urgenti. Non è consentito durante l'orario di lavoro usare il proprio telefono per accedere alla rete internet, anche se collegata alla propria SIM, e quindi accedere a social network e giochi ed ogni altra applicazione non coerente con i fini lavorativi/istituzionali;

E' vietato utilizzare il telefono per riprendere le attività, specie durante le lezioni con la presenza di minori. E' vietato fare foto/video, trasferire foto/video, anche su social network, si dati aziendali e di minori e di ogni soggetto scolastico.

Il telefono aziendale, qualora venisse assegnato, è uno strumento di lavoro viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. Un apposito regolamento ne disciplinerà l'utilizzo.

**ART 15 DIRITTI E RESPONSABILITÀ DEI DIPENDENTI**

Per assicurare la tutela dei diritti, delle libertà fondamentali e della dignità dei lavoratori, garantendo che sia assicurata una ragionevole protezione delle loro sfera di riservatezza nelle relazioni personali professionali, il trattamento dei dati mediante l'uso delle tecnologie telematiche è conformato al rispetto dei diritti delle libertà fondamentali nonché della dignità dell'interessato, dei divieti posti dallo statuto dei lavoratori sul controllo a distanza e dei principi di necessità, correttezza e finalità determinate, esplicite e legittime. Ogni utente è responsabile, sia sotto il profilo civile che penale, del corretto uso delle risorse informatiche, dei servizi e dei programmi ai quali ha accesso e dei dati che tratta. Spetta ai docenti vigilare affinché gli studenti loro affidati rispettino il regolamento e sono ne direttamente responsabili.

**ART. 16 DOVERI DI COMPORTAMENTO DEI DIPENDENTI**

Le strumentazioni informatiche, la rete internet e la posta elettronica devono essere utilizzate dal personale e dagli studenti sotto il controllo dei loro docenti, come strumenti di lavoro e studio. Ogni loro utilizzo non inerente l'attività lavorativa e di studio è vietato in quanto può comportare disservizi, costi di manutenzione e soprattutto minacce alla sicurezza. In particolare non può essere dislocato nelle aree di condivisone della rete alcun file che non sia legato all'attività lavorativa, nemmeno per brevi periodi. Agli utenti è severamente vietata la memorizzazione di documenti informatici di natura oltraggiosa o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinioni, appartenenza sindacale politica. Non è consentito scaricare, scambiare o utilizzare materiale coperto dal diritto d'autore.

## ART 17 CONTROLLI E SANZIONI

Il datore di lavoro, per esigenze organizzative, per garantire la sicurezza sul lavoro, per evitare reiterati comportamenti dolosi illeciti può avvalersi legittimamente, nel rispetto dell'art. 4 comma 2 dello statuto dei lavoratori, di sistemi che consentano un controllo a distanza e determinato di dati personali riferibili a singoli utenti. La lettura e la registrazione sistematica del servizio di accesso ad internet vengono

automaticamente registrate. Tali file possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente. Le registrazioni possono essere utilizzate per fornire informazioni esclusivamente su: numero di siti visitati da ciascun utente, quantità totale di dati scaricati, postazioni di lavoro utilizzate per la navigazione.

Qualora i controlli evidenzino un utilizzo anomalo degli strumenti informatici dell'istituto, il Titolare e/o il Responsabile del trattamento procede in forma graduata: in via preliminare si eseguono controlli su dati aggregati, in forma anonima e si provvede ad un avviso generalizzato agli utenti, se perdurano le anomalie si procede a controlli per tipologie di locali di utilizzo (uffici, aule, ...) o tipologie di utenti (ATA, docenti, studenti, ...) e si procede con avvisi mirati alle categorie di utilizzatori, ripetendosi l'anomalia, sarà lecito il controllo su base individuale e si procederà all'invio di avvisi individuali, in caso di verificato e reiterato uso non conforme delle risorse informatiche il Titolare del Responsabile del trattamento attiva il procedimento disciplinare nelle forme e con le modalità previste dall'istituto per gli studenti (vedere Regolamento di Istituto e di disciplina), dai contratti di lavoro per i dipendenti e attraverso l'adozione degli atti di specifica competenza nel caso di personale non dipendente, può portare alle azioni civili e penali consentite. L'utilizzo dei servizi di accesso ad internet cessa o viene sospeso d'ufficio quando: non sussiste più la condizione di dipendente/studente o l'autorizzazione al loro uso, vi è il sospetto di manomissione dell'hardware o del software, in caso di diffusione o comunicazione a terzi da parte del dipendente di password, codici di accesso ecc. ..., in caso di accesso doloso a file o servizi non rientranti tra quelli autorizzati, ogni qualvolta sussistano ragionevoli evidenze di una violazione degli obblighi dell'utente che mette a rischio il sistema. Chiunque fosse a conoscenza di comportamenti discordanti da quanto indicato nel presente regolamento ha l'obbligo di informare il Titolare, il Responsabile del Trattamento dei dati e l'Amministratore di Sistema al fine di limitare eventuali abusi. L'Istituto, in ogni caso, non sarà responsabile per le condotte illecite poste deliberatamente in essere dagli utenti del servizio.

## ART. 18 INFORMATIVA AGLI UTENTI

Il presente regolamento è messo a disposizione degli utenti, per la consultazione, sui mezzi di comunicazione interna utilizzati dall'istituto (circolare, sito) e quindi portato a conoscenza di ciascun dipendente. L'utente qualora l'istituto decidesse di perseguire, per fini legati alla sicurezza dell'intero sistema informativo, il controllo della posta elettronica e della navigazione in internet, viene informato degli strumenti e dei modi di trattamento effettuati prime che questo sia iniziato.

## ART. 19 PUBBLICITA'

Copia del presente Regolamento è pubblicato sul sito dell'Istituzione Scolastica

## ART. 20 DISPOSIZIONI FINALI

Per quanto non previsto dal presente Regolamento si applicano le norme contenute nelle vigenti disposizioni nazionali