ISTITUTO STATALE DI ISTRUZIONE SECONDARIA
"Leonardo DA VINCI"
Via Filippo TURATI – 80040 Poggiomarino NA – Tel/Fax.0815281440
NAIS1019006@ISTRUZIONE.IT - ***NAIS019006@PEC.ISTRUZIONE.IT***
www.isisleonardodavincipoggiomarino.it

Poggiomarino (NA), 13-10-2020

Regolamento per l'utilizzo della rete informatica

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 GDRP;
- 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;
- 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 è aggiornato con cadenza annuale, 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.

POGGIOMARINO, 13/10/2020

La DIRIGENTE SCOLASTICA
Titolare del Trattamento dei dati
Prof.ssa Olimpia Maria Tiziana SAVARESE
Documento firmato digitalmente ai sensi del c.d. Codice dell'Amministrazione Digitale e normativa connessa

Regolamento per l'utilizzo della rete informatica

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 maggiori 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 alle reali utilizzi quotidiano 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 dell'Istituto ISIS "Leonardo Da Vinci" 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.

ART. 2 PRINCIPI GENERALI – DIRITTI E RESPONSABILITÀ

- L'Istituto ISIS "Leonardo Da Vinci" 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 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 di alunni, ne 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;

- 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 web, intranet, bacheche, etc)

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 ed 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) al *personal computer* di ciascuno.
- 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 la relativa *password*.
- 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 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.
- Su ogni computer e server deve essere installato un software antivirus e le firme per identificare nuovi virus devono essere aggiornate frequentemente. 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.

- È vietato modificare le caratteristiche impostate sul proprio *PC*, salvo autorizzazione esplicita dell'Amministratore di Sistema o del Dirigente Scolastico.
- 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, chiavi USB, 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 Dirigente Scolastico, 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:
    1. Lunghezza minima: 8 caratteri
    2. Complessità: utilizzo di caratteri speciali, almeno una maiuscola, almeno un numero
    3. Durata: la password deve avere una scadenza non più lunga di 90 giorni
    4. 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.**
- Si parte quindi dal presupposto che **i *file* relativi alla produttività individuale vengono salvati sul *server*** e i limiti di accesso sono regolarizzati da apposite procedure 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, 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. Il responsabile dell'amministrazione potrà autorizzare l'utilizzo momentaneo delle *password*, all'assistente amministrativo che sostituisce il titolare responsabile del settore lavorativo, anche se per breve periodo e provvedere alla creazione dell'utente nuovo.

- 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.
- 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.
- 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 componenti hardware non compatibili con l'attività istituzionale;
5. rimuovere, danneggiare o asportare componenti hardware;
6. modificare i collegamenti della strumentazione o effettuarne di nuovi senza il consenso dei responsabili del laboratorio e/o dell'Amministratore del Sistema;
7. 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;
8. 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;
9. 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. È un bene comune e con performance bilanciate in base al carico di utilizzo, pertanto il relativo utilizzo 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. 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 cui si espongono collegandosi alla rete, riconoscendo ed evitando gli aspetti negativi (pornografia, violenza, razzismo …).
- 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

1. 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;
2. una back-list di siti non visitabili, casomai utilizzando degli appostiti filtri dei contenuti che filtrano le pagine in base al contenuto;

ART. 6 UTILIZZO DELLA POSTA ELETTRONICA

- La casella di posta, assegnata dall'Istituto, è uno strumento di lavoro e le persone assegnatarie delle caselle di posta elettronica sono responsabili del loro corretto utilizzo.
- 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.
- 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:

1. 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);

2. l'apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell'identità del mittente;
3. inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici.
4. Modificare la password della posta elettronica almeno ogni 6 mesi;

ART. 7 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 Dirigente Scolastico. 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 Dirigente Scolastico 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. 8 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. 9 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, etc), in caso di allontanamento devono essere custoditi in un luogo protetto.

ART. 10 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. È 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. È buona norma programmare la stampante in modo da generare un file non di grandi dimensioni, così da poter inviare anche mediante posta elettronica.

ART. 11 REATI E VIOLAZIONI DI LEGGE

- Al di là delle regole di buona 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. 12 AMMINISTRATORE DI SISTEMA

- 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:

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 Dirigente Scolastico;
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 Dirigente Scolastico, 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. 13 NON OSSERVANZA DEL REGOLAMENTO

- Si raccomanda il rispetto delle regole contenute nel presente regolamento da parte degli utenti il mancato rispetto o violazione comporterà la revoca delle autorizzazioni e le necessarie conseguenze secondo la normativa vigente, per quanto non previsto nel presente regolamento valgono le disposizioni normative e legislative vigenti.
- 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. 14 SANZIONI

- A fronte di violazioni accertate delle regole stabilite dal presente regolamento, l'Istituto, su valutazione del responsabile di laboratorio e del Dirigente Scolastico e dell'Amministratore di Sistema, si assume il diritto di impedire l'accesso dell'utente a Internet per un certo periodo di tempo, in rapportato alla gravità del reato.
- La violazione colposa o dolosa accertata delle norme del presente regolamento, oltre all'intervento disciplinare del docente e/o del consiglio di classe, potrà dare luogo alla richiesta di risarcimento delle ore perse per ripristinare il sistema e renderlo nuovamente operante ed affidabile, oltre che del danno anche d'immagine. Rimangono comunque applicabili ulteriori sanzioni disciplinari, eventuali azioni civili per danni, nonché l'eventuale denuncia del reato all'Autorità Giudiziaria.
- Nel caso di infrazione consapevole da parte dei docenti o del personale non docente, sarà in ogni caso compito del Dirigente Scolastico intervenire per via amministrativa secondo le norme vigenti.

Art. 15 UTILIZZO LABORATORI DIGITALI – LABORATORI DI INFORMATICA

- Le chiavi dei laboratori digitali e laboratori di informatica vanno custodite dal DSGA. Il ritiro e la riconsegna delle chiavi sono di competenza del docente che utilizza il laboratorio.
- L'insegnante avrà cura, all'inizio ed alla fine di ogni lezione, di verificare l'integrità di ogni singola postazione e di ogni singolo strumento utilizzato.
- L'insegnante di classe che ha nella propria programmazione l'utilizzo di Internet è responsabile di quanto avviene nelle proprie ore di laboratorio.
- L'insegnante, qualora alla fine della lezione dovesse rilevare danni, manomissioni alle attrezzature è tenuto a darne tempestiva comunicazione al Dirigente Scolastico e al DSGA.
- L'accesso delle classi ai laboratori deve essere regolamentato dall'osservanza della tabella oraria compilata da tutti i docenti interessati all'utilizzo dei PC o di altra strumentazione.

- L'utilizzo dei laboratori di informatica comporta la puntuale compilazione del registro delle presenze, sul quale è obbligatorio annotare eventuali anomalie/malfunzionamenti dei dispositivi hardware e dei software.
- Sarà compito dell'amministratore di Sistema e dei Tecnici dei laboratori procedere con l'inventario dei bani strumentali (hardware e software) delle licenze d'uso e dei manuali e driver di sistema.
- Gli Studenti devono attenersi alle seguenti indicazioni:

1. È vietato introdurre bevande all'interno dei laboratori di informatica durante l'utilizzo dei computer e/o delle stampanti.
2. Gli studenti non possono usare i computer in rete senza l'ausilio e il coordinamento del docente.
3. Non utilizzare giochi né in locale, né in rete;
4. Salvare sempre i lavori propri (file) in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento delle macchine cancellare file di lavoro sparsi per la macchina e al di fuori delle cartelle personali;
5. Mantenere segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della vostra scuola;
6. Non inviare a nessuno fotografie personali o di propri amici, nè di personale della scuola (Dirigente, Docenti, Collaboratori, Amministrativi, Esperti Esterni);
7. Chiedere sempre al Docente il permesso di scaricare documenti da Internet;
8. Chiedere sempre l'autorizzazione al Docente prima di iscriversi a qualche concorso o prima di riferire l'indirizzo della propria scuola;
9. Riferire immediatamente al Docente nel caso in cui qualcuno invii immagini inappropriate od offensive. Non rispondere, in ogni caso, al predetto invio;
10. Riferire all'insegnate in caso di reperimento di immagini inappropriate od offensive durante la navigazione su Internet;
11. Riferire al Docente, o comunque ad un adulto, qualora qualcuno su Internet chieda un incontro di persona;
12. Ricordarsi che le persone che si "incontrano" nella Rete sono degli estranei e non sempre sono quello che dicono di essere;
13. Non è consigliabile inviare mail personali, perciò rivolgersi sempre all'insegnante prima di inviare messaggi di classe;
14. Non caricare o copiare materiale da Internet senza il permesso dell'insegnante o del responsabile di laboratorio.
15. È vietato a chiunque non sia autorizzato installare programmi, modificare installazioni di programmi e di rete, cambiare le configurazioni delle macchine

- L'assistenza per piccoli interventi è assicurata dal personale aiutante tecnico disponibile, che svolge le proprie mansioni di collaborazione e assistenza nei laboratori coadiuvato dall'Amministratore di Sistema al fine di garantire l'efficienza dei locali e delle attrezzature e lo svolgimento regolare delle attività didattiche.
- Ad ogni laboratorio è assegnato il personale tecnico di riferimento, che all'inizio delle lezioni si assicurerà dell'accensione e del corretto funzionamento delle macchine ed alla fine delle lezioni

parteciperà all'accertamento della situazione del materiale e attrezzature e di eventuali anomalie o mancanze ed accerterà, inoltre, che siano spente tutte le apparecchiature nonché l'interruttore generale e che l'aula sia lasciata in condizione adeguata per ricevere un'altra classe.

- La rete informatica dei laboratori e in generale delle diverse aule che utilizzano le LIM ed altri strumenti connessi alla rete deve essere distinta dalla rete utilizzata dai PC della segreteria didattica, visto che in quest'ultima circolano dati personali e sensibili da proteggere.
- Per guasti che richiedono l'intervento dell'assistenza tecnica esterna, il personale assistente tecnico richiederà per iscritto l'intervento delle ditte incaricate, spegnendo gli interruttori e lasciando l'attrezzatura in questione inattiva, apponendo il cartello di "fuori servizio".
- I laboratori devono essere dotati di estintori portatili di tipo approvato in stato di efficienza. Per spegnere incendi di origine elettrica o prossimi a impianti elettrici sotto tensione non si deve usare acqua, ma gli appositi estintori possibilmente del tipo a CO2.
- Il firewall potrebbe gestire, con le regole sopra citate, entrambe le reti, così da creare delle sotto-reti logiche di un unico cablaggio strutturato.
- Il firewall, qualora possibile, potrà anche gestire 2 reti WAN, configurate in bilanciamento di carico, dando eventualmente un peso maggiore alla rete della segreteria rispetto alla rete della didattica.

Art. 15 SITO WEB DELLA SCUOLA E SERVIZI ON-LINE ALLE FAMIGLIE, STUDENTI, DOCENTI/UTENTI ESTERNI

- Sarà cura dell'Amministratore di Sistema o qualora individuato il Responsabile (webmaster) 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 con il consenso dei loro genitori. Le fotografie degli studenti per il 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. 16 WIFI

L'Istituto è dotato di diversi hotspot per la connessione Wifi 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 WiFi, registrando nell'apposita lista il MAC address.

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

ART. 17 UTILIZZO DI TELEFONINI E ALTRE APPARECCHIATURE DI REGISTRAZIONE DI IMMAGINI E SUONI

- È fatto divieto assoluto di effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi, salvo:
    - diversa disposizione esplicita del titolare del trattamento, da concordarsi di volta in volta e comunque sempre preventivamente al trattamento;
    - informazione preventiva degli interessati;
    - acquisizione del loro libero consenso, preventivo ed informato.

ART. 18 AGGIORNAMENTO E REVISIONE

- Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Il presente Regolamento è soggetto a revisione con frequenza annuale o in caso di variazioni della normativa vigente.