REGOLAMENTO SULLA POLITICA DI USO ACCETTABILE DELLA RETE E DELLE RISORSE DIGITALI (P.U.A.)

REVISIONE 1.0 – A.S. 2020-2021

Il curricolo scolastico prevede l'utilizzo di strumentazioni informatiche (*PC, tablet, stampanti, …*) con cui gli studenti potranno svolgere le normali attività, reperire materiale, elaborare documenti e scambiare informazioni utilizzando le Tecnologie per l'Informazione e la Comunicazione (TIC).

Per docenti e studenti l'accesso a risorse e servizi internet da scuola, nel rispetto delle disposizioni del Ministero dell'Istruzione Università e Ricerca, è consentito esclusivamente per uso didattico.

La Politica per l'Uso Accettabile della rete fornisce le linee guida per il benessere e la sicurezza di tutti gli utenti della rete; il suo scopo è promuovere le competenze digitali ed un uso delle TIC positivo, critico e consapevole, sia da parte degli alunni che degli adulti coinvolti nel processo educativo.

Il Regolamento si applica a studenti, docenti e collaboratori scolastici, ciascuno per quanto di sua competenza.

REDAZIONE	VERIFICA	APPROVAZIONE
Data 25/10/2020	*Data 29/10/2020*	*Data 04/11/2020*
Dirigente Scolastico Animatore Digitale	Collegio Docenti	Consiglio di Istituto

1. NATURA E FINALITÀ DEL PRESENTE REGOLAMENTO

La trasformazione digitale in corso, innescata da internet e oggi caratterizzata dalla progressiva e costante diffusione di servizi digitali sempre più evoluti e sempre più pervasivi della nostra vita quotidiana rappresentano sia una grande opportunità che un grave pericolo; la consapevolezza di saper riconoscere gli uni e gli altri richiede un grande sforzo sia da parte della scuola che di tutti i soggetti educatori coinvolti, e una solida alleanza sui principi dell'uso lecito e corretto di tali risorse.

Inoltre il curricolo scolastico e le recenti disposizioni in materia di Didattica Digitale Integrata suggeriscono utilizzo di strumentazioni informatiche, applicazioni e servizi digitali in cloud per integrare ed arricchire le attività didattiche, fino a sostituirle in caso di chiusura dell'Istituto.

Le direttive ministeriali si limitano a stabilire che l'uso in classe dei dispositivi digitali è consentito esclusivamente a scopo didattico, vietando ogni altra finalità. Questo regolamento vuole fornire alcune linee guida per un uso equo, consapevole e sicuro della rete e delle risorse digitali.

2. RISORSE DIGITALI OGGETTO DEL REGOLAMENTO

a) Il **Registro Elettronico** Argo (RE).
Tramite RE i soggetti in possesso delle credenziali fornite dalla scuola possono condividere materiale; l'uso del servizio è regolamentato a parte ma nel condividere materiali tutti dovranno attenersi alla PUA.

b) La piattaforma **G Suite**.
Tramite G Suite i soggetti in possesso delle credenziali fornite dalla scuola possono condividere materiale; l'uso del servizio è regolamentato a parte ma nel condividere materiali tutti dovranno attenersi alla PUA.

c) **Laboratori** scolastici.
Nei laboratori didattici vengono messi a disposizione postazioni di lavoro; l'uso di ogni laboratorio è regolamentato a parte ma durante lo svolgimento delle attività tutti dovranno attenersi alla PUA.

d) Dispositivi vari.
Nelle aule e nei locali di servizio sono a disposizione postazioni di lavoro fisse e mobili, sia ad uso collettivo, sia concesse, in comodato, per uso individuale; l'uso di ciascuno è regolamentato a parte ma durante lo svolgimento delle attività tutti dovranno attenersi alla PUA.

e) Dispositivi personali.
Ai docenti è consentito l'accesso alla rete della scuola tramite dispositivi personali purché a scopo didattico; l'uso dei dispositivi personali è regolamentato a parte ma durante lo svolgimento delle attività tutti dovranno attenersi alla PUA.

È VIETATO QUALSIASI UTILIZZO NON CONFORME ALLA P.U.A.

3. PREMESSA

Premesso che ogni servizio internet ha le sue specifiche policy in tema di come e cosa pubblicare, ci si riferisce al termine Netiquette, nel linguaggio della rete, per indicare un insieme di regole informali che disciplinano il buon comportamento nel rapportarsi con gli altri tramite tecnologie digitali. È opportuno che tutti le conoscano per un uso consapevole e responsabile delle TIC.

Queste regole sono le linee guida fondamentali per la sicurezza e il benessere di tutti nella rete, in particolare negli ambienti più usati dagli adolescenti. Tutti gli utenti della rete e delle risorse digitali dell'Istituto devono rispettare scrupolosamente questi principi, le leggi vigenti in materia di diritto d'autore e tutela della privacy nonché le specifiche norme penali relative al settore informatico e della comunicazione elettronica, oltre ad ogni altra disposizione generale di legge.

4. PRINCIPI GENERALI

a) I principali servizi internet e il WWW in particolare favoriscono collaborazione, condivisione e libertà d'espressione, ma è necessario sapere che di queste risorse può essere fatto un uso malevolo e/o illecito e che sono reperibili anche contenuti illeciti e/o pericolosi.
b) I servizi internet sono spesso utilizzati da malintenzionati per diffondere malware (*software malevolo come virus, worm, ransomware, …*) da cui è importante proteggersi tenendo regolarmente aggiornati tutti i software, utilizzando specifiche applicazioni per la sicurezza (*antivirus, firewall, …*) e adottando comportamenti prudenti in generale e, specialmente, evitando di attivare link o aprire file di origine dubbia.
c) Le identità digitali di molti servizi internet non sono identità verificate; usando questi servizi è facile imbattersi in identità false o gestite da BOT; diffidate delle identità virtuali di cui non avete una diretta conoscenza nel mondo reale.
d) Quando, in linea generale e nel proprio quotidiano, si utilizzano i Social Network, servizi web o altre applicazioni internet (*YouTube, Facebook, Instagram, Twitter, WhatsApp, Telegram, Netlog, Tik Tok, etc.*), è molto importante informarsi su quali siano i diritti e i doveri dell'utente, leggendo attentamente la licenza d'uso e l'informativa sul trattamento dei dati personali, tenendosi regolarmente aggiornati sulle periodiche revisioni di tali documenti.
e) Esiste un regolamento europeo (GDPR) che disciplina e tutela i dati personali e la privacy; la pubblicazione e condivisione di dati personali o, peggio, dati sensibili è consentita solamente se si ha la certezza che tali informazioni vengano rese note esclusivamente ai soggetti autorizzati e che la trasmissione avvenga tramite canali sicuri. Se si decide di condividere informazioni personali, bisogna scegliere con cura che cosa rendere pubblico e cosa rendere privato, facendo particolare attenzione alle impostazioni di visibilità che i servizi mettono a disposizione, evitando di dare accesso a soggetti sconosciuti o non verificati. Nei social scegliete con cura i contatti a cui dare l'accesso al vostro profilo e i gruppi a cui aderire.

f) Proteggete con cura la vostra identità digitale: utilizzate password robuste (*https://support.google.com/accounts/answer/32040?hl=it*); abilitate i servizi di sicurezza (*autenticazione a due fattori*) e verificate regolarmente gli accessi al vostro account. Se attivate il recupero della password con domanda segreta, siate certi di utilizzare domande dalla risposta non banale.

g) Se si decide di condividere foto, video o qualsiasi altra informazione che riguardano più persone è necessario avere il permesso di ciascun soggetto coinvolto prima di effettuare la pubblicazione. Se i soggetti sono minori è necessario anche il consenso dei genitori/tutori. È vietato pubblicare foto e/o video fatti di nascosto e dove sono riconoscibili persone riprese senza il loro consenso. Nella produzione di materiali multimediali ricorrete a strategie di ripresa che non rendano riconoscibili i soggetti se volete evitare di dover raccogliere i consensi.

h) In nessun caso è consentita la pubblicazione, con qualsiasi mezzo, di contenuti lesivi della dignità umana e delle minoranze, che contengano incitamento all'odio (*hate speech*) basato sulla razza, sul sesso, sulla religione o sulla nazionalità, nonché di contenuti ritenuti potenzialmente lesivi dello sviluppo fisico, psichico o morale dei minori, o che presentano scene di violenza gratuita, insistita, efferata o pornografiche.

i) Il web è un luogo libero e accessibile a chiunque ed è responsabilità di tutti contribuire a renderlo un luogo sicuro e di sviluppo sociale; ogni volta che un contenuto o un comportamento scorretto e involontario viene rilevato dobbiamo impegnarci ad avvisare l'autore fornendogli le informazioni utili a capire l'errore, contribuendo così a diffondere i principi dell'uso sicuro, consapevole e responsabile delle TIC.

j) Ogni abuso subito o rilevato nell'uso di applicazioni e servizi internet deve essere segnalato tramite i canali e gli strumenti offerti dal servizio stesso, indicando in modo chiaro e semplice i riferimenti per ottenere tempestivamente la rimozione del contenuto (*abuso, data, ora, utenti e servizio coinvolti*). Quasi tutti i servizi internet e, in particolare, tutti i social network garantiscono la possibilità di segnalare materiale inopportuno; le informazioni specifiche per la segnalazione sono facilmente reperibili sul sito web del fornitore del servizio o tramite motore di ricerca. Se il fatto poi costituisce reato è necessario che venga segnalato alle autorità competenti.

k) Il MIUR ha messo a disposizione un portale (Generazioni Connesse) per la formazione e il supporto di scuole, docenti, famiglie e alunni; ci sono documenti, risorse e iniziative che meritano di essere diffuse e conosciute da parte di tutti, utenti e operatori della scuola.
WWW.GENERAZIONICONNESSE.IT

l) Utilizzate sempre un software di sicurezza e aggiornatelo regolarmente; aggiornate regolarmente anche il sistema operativo e le applicazioni scaricate. Se possibile adottate per i vostri figli un software di protezione per minori che sia in grado di filtrare i contenuti e configuratelo secondo le vostre necessità.

m) Non disabilitale la protezione del sistema operativo sui dispositivi (*jailbreak*, *rooting*).

n) Non installate applicazioni provenienti da fonti non ufficiali se non siete più che certi della loro natura e provenienza.

o) Verificate regolarmente le impostazioni della privacy delle vostre identità digitali per assicurarvi che il livello di visibilità consentito a chi entra in contatto con voi sia quello desiderato. Disattivate i servizi non necessari.

p) Le applicazioni che installate sul vostro smartphone/tablet potrebbero accedere ai vostri contatti, alla fotocamera, alla posizione, al microfono e a molte altre informazioni personali;

verificate accuratamente che ogni applicazione installata abbia attivati solo gli accessi necessari al suo funzionamento per minimizzare il rischio di abusi.

q) Su dispositivi di uso collettivo, disconnettiti sempre dalle tue identità digitali prima di lasciare la postazione.

r) La capacità di trasporto della rete internet non è infinita, non sprechiamo la banda inutilmente.

5. COMPORTAMENTI NELLE RELAZIONI TRA PARI

a) Tramite e-mail, social network, chat, forum e, più in generale, qualsiasi strumento digitale di comunicazione si instaurano numerose relazioni tra singoli e/o gruppi di utenti, non veicolate o controllate da intermediari, chiamati relazioni di pari livello. È importante fare attenzione a quali informazioni vengono fornite in questo contesto, evitando di condividere dati personali e di contatto, come numeri di telefono o indirizzi, che nella vita reale non si darebbero a persone che non sono ancora degne di fiducia.

b) Bisogna evitare di scambiare contenuti di ogni genere con soggetti sconosciuti o di cui non ci si può fidare e, anche quando si conosce l'interlocutore, è fondamentale un atteggiamento prudenziale nei confronti dei link o dei file che vengono scambiati in quanto potenzialmente pericolosi; prima di accedervi assicuratevi che il dispositivo che state usando sia aggiornato e adeguatamente protetto da un software di sicurezza (*antivirus*).

c) Se durante una chat, un forum o una qualsiasi discussione online, l'interlocutore diviene volgare, offensivo o minaccioso, si deve evitare di fomentarlo, ignorandolo e abbandonando la conversazione.

d) Quando si riscontra un comportamento riconducibile ad un illecito durante una conversazione privata, (*un tentativo di approccio sessuale a minori, stalking, cyberbullismo, hate speech, …*) l'utente deve segnalarlo tempestivamente tramite i sistemi predisposti all'interno del servizio, indicando in modo chiaro e semplice i riferimenti (*nickname, informazioni temporali, screenshot, …*) utili ad identificare e fermare l'abuso. Se il caso lo richiede la segnalazione va anche fatta alle autorità competenti in materia. Molti servizi internet vi consentono di bloccare selettivamente gli utenti, sfruttate questa opzione per liberarvi dei contatti indesiderati e/o inopportuni. Se non sapete come fare fatevi aiutare da un adulto esperto. Nei casi più gravi può essere utile abbandonare non soltanto la conversazione ma anche disattivare e/o eliminare il proprio profilo personale su quel servizio.

e) Nelle conversazioni di gruppo, siano esse via mail, social, chat o altro servizio, è necessario tutelare la privacy di tutti mascherando e/o eliminando le informazioni personali dei soggetti coinvolti quando non si conoscono tra di loro. Se un servizio non offre questa possibilità, prendete in considerazione la possibilità di cambiare strumento per gestire la conversazione.

f) Tutte le opere dell'ingegno e dunque anche i contenuti reperibili tramite i diversi servizi internet sono tutelati dal diritto d'autore; riprodurre, scambiare o pubblicare contenuti protetti da copyright senza averne diritto è sanzionabile dalla legge ed è irrispettoso nei confronti del creatore. Non fatelo.

g) Non bisogna diffondere file o contenuti se non si ha la certezza che tale comportamento sia lecito, adeguato e che non rappresenti un pericolo per il destinatario e i suoi dispositivi.

h) Applicazioni o file provenienti da internet e scaricati sul proprio dispositivo potrebbero essere potenzialmente pericolosi; prima di accedervi assicuratevi che il dispositivo che state usando sia aggiornato e adeguatamente protetto da un software di sicurezza (*antivirus*).

i) File o altri contenuti scambiati nelle relazioni tra pari potrebbero essere illeciti, ingannevoli o acquisiti illecitamente; prima di accettare file o contenuti assicurarsi della provenienza e dell'affidabilità di colui che li fornisce.
j) Le identità digitali possono essere ingannevoli o perché gestite da software o perché diversa dalla reale identità dell'utilizzatore; è bene evitare di instaurare relazioni con identità digitali non verificate o sospette.
k) Sii chiaro e conciso, prediligi le comunicazioni asincrone (*e-mail, Whatsapp, …*), rispetta i tempi dei tuoi interlocutori.
l) Nelle conversazioni sincrone (*videochat, chiamate, …*) evita di sovrapporti agli altri; disattiva il microfono quando non necessario; evita gli ambienti rumorosi e/o ventosi.
m) Evita termini gergali, abbreviazioni o stili comunicativi poco chiari; non scrivere in maiuscolo (equivale ad urlare); non abusare delle emoticon.
n) Rileggi sempre quello che hai scritto prima di premere il pulsante "pubblica".
o) Ricordati di dire sempre chi sei, non dare per scontato che l'interlocutore capisca al volo con chi sta conversando.
p) Usa la funzione "rispondi" per mantenere la coerenza delle conversazioni; se non puoi evita di dare per scontata la conoscenza del contenuto di precedenti conversazioni.

6. DIFFUSIONE DI CONTENUTI GENERATI DAGLI UTENTI

a) Prima di caricare e condividere contenuti tramite social, chat, forum o qualsiasi altro servizio internet lo consenta è necessario che vi informiate sulla tutela della privacy offerta dal servizio e, in particolare, sulle diverse opzioni di visibilità che potete scegliere per ciò che volete condividere; siate sempre consapevoli di quali utenti della community possono accedere ai contenuti che state pubblicando.
b) Bisogna essere consapevoli che ciò che viene pubblicato tramite social, chat, forum o altro servizio internet è persistente, può essere facilmente riprodotto e distribuito senza il vostro consenso ed è complicato da cancellare. Bisogna evitare di contribuire con materiale che in futuro non si vorrebbe veder pubblicato.
c) Quando si contribuisce con del materiale in un ambiente condiviso, l'utente è tenuto ad essere coerente con il contesto e le regole di fatto della community, evitando di pubblicare materiale inadeguato e che potrebbe risultare fuori contesto.
d) Molti servizi internet sono moderati e/o possiedono dei sistemi automatici di segnalazione/rimozione dei contenuti; se un contenuto che avete pubblicato non è più visibile online, probabilmente non rispetta gli standard del servizio o della community. Consultate le norme di utilizzo del servizio per capire cosa avete sbagliato; provate a modificare linguaggio e riflettete se il servizio usato è davvero il posto migliore per quel tipo di contenuto.
e) Quando si fa uso di etichette (*tag, hashtag)* per catalogare un contenuto/utente, bisogna assicurarsi che l'etichetta sia coerente con il contenuto/utente; quando si vuole taggare una persona è opportuno contattarla preventivamente per ottenere il suo consenso.

7. GESTIONE DELLE RELAZIONI SOCIALI – COMMUNITIES

a) Le relazioni sociali che si sviluppano all'interno delle Communities (*Social network, forum, …*) sono simili a quelle reali, pertanto la fiducia verso i propri contatti deve essere gestita proprio come accade nella realtà.
b) Se si instaura un'amicizia virtuale con persone di cui non si conosce la reale identità, bisogna assicurarsi che il profilo virtuale corrisponda realmente alla persona che lo utilizza. La facilità con cui ci si può imbattere in profili falsi o gestiti da BOT richiede estrema prudenza nella

condivisione di contatti, dati personali e contenuti privati; nel dubbio NON condividete nulla con profili non verificati.

c) La reputazione digitale è persistente e si diffonde velocemente, pertanto non bisogna mai diffamare altre persone, soprattutto se le stesse non sono presenti sul Social Network e non possono accorgersi del danno subito.
d) In molte communities si fa uso di etichette (*tag, hashtag)* per indicizzare i contenuti e indirizzarne la visibilità; usate tali strumenti solo se siete certi di avere il consenso di tutti i soggetti coinvolti.
e) Nel condividere contenuti con una community rispettate la sensibilità, le regole e il linguaggio che la community si è data evitando di pubblicare materiale fuori contesto.
f) Nelle communities con moderatore rispetta le sue scelte e adegua comportamento e linguaggi al contesto; oppure abbandona la community.

8. SICUREZZA E UTILIZZO DELLE TIC

La rete dati, l'accesso a internet, le postazioni di lavoro e i laboratori messi a disposizione della scuola a docenti e alunni sono risorse collettive da tutelare per il bene di tutta la comunità scolastica e pertanto sono soggette a monitoraggio da parte del personale tecnico per verificarne il corretto funzionamento ed utilizzo.

Al fine di garantire una gestione il più possibile corretta, la scuola attua le seguenti strategie:

- Il Dirigente Scolastico si riserva, sentiti i responsabili, di limitare l'accesso e l'uso della rete interna (*Intranet*) ed esterna (*internet*) secondo i normali canali di protezione presenti nei sistemi operativi e utilizzando, se necessario, software/hardware aggiuntivi.
- È fatto divieto a tutti di svolgere le seguenti attività:
  - ✓ Non rispettare le leggi sui diritti d'autore e, in particolare, scaricare contenuti protetti.
  - ✓ Visitare siti non attinenti alla normale attività didattica.
  - ✓ Alterare i parametri di configurazione dei computer in uso.
  - ✓ Utilizzare la risorse messe a disposizione dalla scuola per interessi privati e personali.
  - ✓ Aggirare i meccanismi di protezione attivati dalla scuola.

DISPOSIZIONI, COMPORTAMENTI, PROCEDURE:

- Il sistema informatico è periodicamente controllato dai responsabili e da procedure automatizzate di registrazione e controllo degli accessi.
- La scuola si riserva il diritto di verificare accessi e utilizzo delle risorse messe a disposizione dalla scuola al fine di garantire il buon funzionamento del sistema informatico e a tutela della sicurezza di tutti gli utenti, inclusi i file temporanei e i siti visitati da ogni postazione.
- È vietato scaricare e installare da internet software non autorizzati
- Al termine di ogni utilizzo ogni utente deve assicurarsi di chiudere le sessioni aperte, sia in locale che nei servizi on line, eliminando eventualmente le password memorizzate; è responsabilità di ciascuno evitare che altri utenti dopo di lui possano accedere a strumenti e risorse senza essere riconosciuti semplicemente utilizzando lo stesso dispositivo lasciato incautamente abilitato.
- L'utilizzo di CD, chiavi USB e dispositivi removibili personali sui PC della scuola deve essere autorizzato dal Dirigente solo in casi eccezionali, solo previa scansione antivirus e sotto la responsabilità del docente/ATA che opera su quel dispositivo
- La scuola, allo scopo di tutelare la sicurezza del proprio sistema informatico, si riserva la facoltà di limitare l'accesso a determinate risorse o servizi internet, sia temporaneamente (*per ragioni tecniche*) che in modo permanente (*se incompatibili con l'attività didattica*).

UTILIZZO DEI SERVIZI INTERNET

- ☞ Si raccomanda a docenti e studenti l'uso dell'account istituzionale fornito dalla scuola.
- ☞ L'insegnante di classe, che ha nella propria programmazione l'utilizzo di internet, è responsabile di quanto avviene nelle proprie ore di lezione.
- ☞ È vietato utilizzare le risorse messe a disposizione dalla scuola per uso privato durante le ore di lezione.
- ☞ È vietato l'utilizzo delle postazioni durante le ore di lezione per motivi non strettamente legati alla pratica didattica.

SICUREZZA DELLA RETE INTERNA (LAN)

- ☞ Il collegamento di computer portatili o palmari personali alla rete di Istituto deve essere autorizzato dal Dirigente Scolastico.
- ☞ La rete interna è protetta da Firewall per quanto riguarda le connessioni con l'esterno.

LINEE GUIDA DI UTILIZZO DELLE TIC PER STUDENTI E DOCENTI

STUDENTI:

- ☞ Gli strumenti delle TIC devono essere utilizzati esclusivamente a scopo didattico.
- ☞ Su indicazione dei docenti, salvate sempre i vostri lavori (*file*) sullo storage remoto (*Google Drive*) associato all'account scolastico che vi è stato assegnato. Attenetevi alle disposizioni degli insegnanti e allo specifico regolamento per il corretto utilizzo della piattaforma. In particolare:
  - ✓ Mantenete riservati i vostri dati personali (*nome, indirizzo, n. di telefono, classe frequentata, indirizzo della scuola, …*)
  - ✓ Non inviate a nessuno fotografie vostre o di vostri amici.
  - ✓ Chiedete sempre al vostro insegnante il permesso prima di scaricare contenuti da internet.
  - ✓ Chiedete sempre il permesso prima di iscrivervi a qualche concorso o fornire informazioni su di voi e sulla scuola a soggetti esterni alla scuola.
  - ✓ Riferite sempre al vostro insegnante se ricevete contenuti o immagini che vi infastidiscono; evitate di rispondere a chi vi invia contenuti non adeguati; riferite anche al vostro insegnante se vi capita di trovare questo tipo di contenuti tramite un qualsiasi servizio internet.
  - ✓ Se tramite i servizi internet ricevete inviti ad un incontro di persona, riferitelo al vostro insegnante, alla vostra famiglia o comunque a un adulto di fiducia. Ricordatevi che le identità virtuali in rete possono non corrispondere alle identità reali e che possono essere gestite da malintenzionati e/o software automatici.
  - ✓ Per le attività scolastiche utilizzate sempre l'account fornito dall'istituto.
  - ✓ Non scaricate o copiate contenuti reperibili tramite i servizi internet se non siete più che certi che tali contenuti siano sicuri e non violino le leggi in vigore; in ogni caso dovete sempre avere il permesso preventivo del docente.
  - ✓ Stampate solo dopo aver avuto il permesso del docente; è vietato stampare più copie dello stesso documento; se avete questa necessità stampate solo una copia e rivolgetevi all'ufficio fotocopie per la duplicazione.

DOCENTI

- ✓ Ricordatevi di uscire dal vostro account al termine della sessione di lavoro. Cancellate le password eventualmente memorizzate sulle postazioni di uso comune.
- ✓ Non abusate delle stampanti e stampate solo ciò che è necessario per l'attività didattica; se dovete fare più copie di una stampa, ricorrete all'ufficio fotocopie invece di stampare copie multiple. Valutate la possibilità di distribuire digitalmente il documento invece di stamparlo.
- ✓ Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola.

- ✓ Salvate sempre i vostri lavori (*file*) sullo storage remoto (*Google Drive*) associato all'account scolastico che vi è stato assegnato. Dalle postazioni dedicate alla didattica si deve eliminare qualunque dato alla fine della sessione di lavoro, per ragioni di sicurezza e privacy.
- ✓ Discutete con gli alunni della PUA (*Politica d'Uso Accettabile*) della scuola e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di internet.
- ✓ Date chiare indicazioni su come si utilizza internet, ed eventualmente anche la posta elettronica, e informateli che le navigazioni saranno monitorate.
- ✓ Ricordate agli alunni che le infrazioni saranno sanzionate in riferimento al Regolamento di Istituto e alla normativa vigente.
- ✓ Osservate le indicazioni fornite dal DPO e contenute nel Regolamento sulla Privacy dell'istituzione Scolastica e negli specifici regolamenti dei laboratori.

9. SITO WEB DELL'ISTITUTO

L'Istituto dispone di un proprio sito web e di un proprio dominio. Sul sito della scuola possono venire pubblicate, nel rispetto delle norme vigenti sulla privacy, le informazioni di servizio necessarie al buon funzionamento della scuola, ivi incluse le informazioni di contatto delle persone incaricate dello svolgimento di precise mansioni che prevedono il contatto con il pubblico.

10. VALIDITÀ

Il presente Regolamento entra in vigore a far data dall'approvazione del Consiglio di Istituto e dalla contestuale pubblicazione all'Albo on line-sito web dell'Istituzione Scolastica

11. PUBBLICITÀ E TRASPARENZA

Si dispone la pubblicazione del presente Regolamento all'albo on line, su registro elettronico e sul sito web dell'Istituzione Scolastica.