IISS Majorana-Giorgi

REGOLAMENTO PER L'USO DELLE RISORSE TECNOLOGICHE E DI RETE FINALIZZATE ALL'ATTIVITA' DIDATTICA E AGLI ALUNNI

(approvato dal Consiglio di Istituto nella seduta del 6-12-17)

Riferimenti Normativi

- D.P.R. n. 275 del 25 febbraio 1999;
- L.675 del 31 dicembre 1996 relativa alla privacy;
- C.M. 152/2001 ; 114/2002 sulle diffusione delle reti lan;
- Dlgs 196/2003 T.U. sulla privacy entrato in vigore il 1/1/2004 che riassume le norme precedenti sulla privacy;
- L. 325/2000 sull'adozione delle misure di sicurezza nel trattamento dei dati in applicazione dell'art.15 della L. 675/1996;
- L. 547/ 1993: norme in materia di reati informatici;
- L.4/2004: disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici.
- Raccomandazione del Parlamento Europeo e del Consiglio del 18 /12/2006 (competenza digitale come competenza chiave)
- L. 300/1970, Statuto dei lavoratori

Premessa

Il presente regolamento si propone di:

- garantire la massima efficienza delle risorse,
- garantire la riservatezza delle informazioni e dei dati,
- provvedere ad un servizio continuativo nell'interesse della comunità scolastica,
- provvedere ad un'efficiente attività di monitoraggio,
- garantire il rispetto delle leggi in materia di utilizzo delle risorse informatiche,
- garantire la massima sicurezza nell'interazione tra l'ITIS "MAJORANA-GIORGI"e gli altri soggetti pubblici o privati e ottimizzare i costi di esercizio

Le apparecchiature e i dispositivi elettronici di proprietà esclusiva dell'IISS "MAJORANA-GIORGI"di Genova costituiscono strumenti di lavoro. Tale apparecchiature possono essere impiegate esclusivamente per lo svolgimento delle attività didattiche ed amministrative, funzionali alla gestione della scuola. Referenti e responsabili di apparecchiature elettroniche, piattaforme, siti web di proprietà e in dotazione dell'Istituto devono immediatamente segnalare al D.S. eventuali anomalie, perdite di dati, furti, danneggiamenti o manomissioni.

Il curricolo scolastico nazionale prevede che gli alunni apprendano a ricercare materiale, recuperare documenti e scambiare informazioni utilizzando le TIC (Tecnologie di Comunicazione Informatica).

Gli insegnanti hanno la responsabilità di guidare gli alunni nelle attività on-line, di stabilire obiettivi chiari nell'uso della rete Internet e delle risorse ad essa connesse, nonché di favorire un uso accettabile e responsabile della rete. L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, in relazione al curricolo scolastico, all'età e alla maturità degli alunni.

Il personale di segreteria, nella gestione degli aspetti didattici ed educativi dell'Istituto fa largo uso oramai da anni delle tecnologie informatiche, nell'ottica della dematerializzazione degli atti oltre che per una efficiente ed efficace comunicazione.

Pertanto, al fine del corretto utilizzo delle ICT nonché nell'ottica di una gestione efficiente ed efficace di tutto l'Istituto si rende necessario individuare tutte le risorse tecnologiche informatiche di cui l'Istituto dispone e regolamentarne il loro utilizzo.

Art.1 Infrastrutture tecnologiche

L'IISS "MAJORANA - GIORGI"di Genova dispone di tecnologie informatiche sia per lo svolgimento delle attività didattiche e laboratoriali che per il funzionamento amministrativo. L'Istituto dispone di due reti logicamente separate, utili per l'accesso a internet ed intranet, rispettivamente per l'aspetto amministrativo e didattico.

Art.2 Tutela della privacy

2.1 Tutela della privacy: garanzie generali

Tutte le operazioni relative all'uso della rete sono improntate alla funzionalità nel rispetto della tutela della privacy. Relativamente alla "tutela della persona ed altri soggetti rispetto al trattamento dei dati personali" si fa riferimento al Documento Programmatico sulla Sicurezza con l'indicazione delle persone preposte. La titolarità del trattamento dei dati personali è esercitata dal Dirigente Scolastico. Il Dirigente scolastico designa il responsabile del trattamento dei dati nella persona del DSGA. Per l'attività amministrativa sono state adottate le misure minime, secondo quanto previsto dal D.L. 196/2003: password, codice identificativo personale per ogni utente; programmi antivirus; protezione (firewall) e regolamentazione degli accessi ai locali che ospitano i dati riservati o in cui si trovano le postazioni di lavoro; criteri per garantire l'integrità e la trasmissione sicura dei dati, backup periodici e disaster recovery. Il database non è accessibile dall'esterno: le informazioni gestite non sono fisicamente accessibili dall'esterno, ovvero la loro fruizione è possibile solo dall'interfaccia utente del programma alla quale possono collegarsi solo utenti registrati. Non esistono parti non sottoposte a criteri di sicurezza, l'unico punto di accesso al sistema è la maschera iniziale che richiede l'inserimento di username e password Più utenti possono accedere al sistema contemporaneamente, ma ciascuno opererà in una propria sessione di lavoro indipendente dalle altre. L'utilizzo del registro elettronico da parte dei Docenti, comporta l'integrale applicazione del presente regolamento.

2.2 Tutela della privacy: norme concernenti il personale della scuola

I voti del professore sono privati e consultabili solo dai genitori o dai docenti del Consiglio di classe di appartenenza. Ogni docente per entrare nella piattaforma (registro elettronico) deve obbligatoriamente inserire i suoi personali username e password; Non possono essere presenti due utenti con la stessa username E' assolutamente vietato cedere password, ovvero consentire ad altri soggetti di effettuare operazioni in nome e per conto del titolare di una password. Nell'ipotesi di conoscenza accidentale di dati e/o informazioni riguardanti altri soggetti (alunni, famiglie, docenti e altro personale o non della scuola) è assolutamente vietata la divulgazione, pubblicazione o qualsiasi altra operazione. La mancata osservanza di tali disposizioni darà luogo alle sanzioni previste per legge.

2.3 Tutela della privacy: norme concernenti famiglie e studenti.

Studenti e famiglie possono consultare solo voti e informazioni riguardanti il soggetto interessato. Ogni studente o genitore per entrare nel sistema deve obbligatoriamente inserire i suoi personali username e password; Non possono essere presenti due utenti con la stessa username E' assolutamente vietato cedere password, ovvero consentire ad altri soggetti di effettuare operazioni in nome e per conto del titolare di una password. Nell'ipotesi di conoscenza accidentale di dati e/o informazioni riguardanti altri soggetti (alunni, famiglie, docenti e altro personale o non della scuola) è assolutamente vietata la divulgazione, pubblicazione o qualsiasi altra operazione. La mancata osservanza di tali disposizioni darà luogo alle sanzioni previste per legge

Art. 3 Postazioni informatiche e rete di Istituto generalità

L'accesso alla rete wireless é protetto da misure di sicurezza legate, per il personale della scuola, ad una password e contestuale correlazione univoca con specifiche apparecchiature registrate sotto la propria responsabilità.

Per accesso di ospiti e studenti si utilizza un sistema di accreditamento tramite assegnazione temporanea di credenziali personali su richiesta degli insegnanti o del dirigente scolastico.

E' fatto obbligo, da parte del personale, di comunicare l'eventuale cessione dei propri dispositivi o la dismissione degli stessi in modo da mantenere, da parte dei gestori, di un archivio aggiornato dei dispositivi a cui è consentito l' accesso.

Per accedere alla rete wireless deve dunque essere utilizzata la propria specifica apparecchiatura, sotto la propria responsabilità. E' fatto divieto di utilizzare la rete dell'Istituto per finalità non previste dal presente regolamento o non espressamente autorizzate.

La navigazione è consentita nel rispetto delle seguenti condizioni:

1. è vietato connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del D.S. o del responsabile del Settore indicato dal DS;

2. è vietato monitorare ciò che transita in rete se non nelle forme e nei limiti previsti nel presente regolamento. Per problemi correlati alla sicurezza della rete locale, l'Istituto dispone di un sistema di controllo, il firewall, che registra traccia di tutte le attività sulla rete; il fine è quello di consentire alla P.S., in caso di necessità, l'individuazione del o dei responsabili di eventuali utilizzi fraudolenti della rete di Istituto, della quale è direttamente responsabile il Dirigente Scolastico; infatti, come definito anche dalle linee guida del Garante, il datore di lavoro (il DS), secondo i poteri a lui affidati dalle norme del codice civile, articoli 2086, 2087 e 2104, può riservarsi di controllare l'effettivo adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro; tuttavia, ciò deve essere fatto nel rispetto delle norme poste a tutela del lavoratore (ci si riferisce, in particolare, al divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" di cui all'art. 4 della legge 300 del 1970). Pertanto il datore di lavoro potrebbe, ad esempio, verificare se vi è stato indebito utilizzo della connessione ad Internet da parte del dipendente attraverso il controllo degli accessi e dei tempi di connessione, senza però indagare sul contenuto dei siti visitati.

3.1 Utilizzo delle postazioni da parte dei docenti

I docenti che utilizzano laboratori e /o postazioni informatiche hanno l'obbligo di vigilare sul corretto utilizzo delle stesse da parte degli studenti sia quando operano singolarmente che in gruppo. In particolar modo ogni docente è tenuto a:

a) illustrare ai propri allievi le regole di utilizzo contenute nel presente documento;

b) controllare che l'accesso degli alunni alla rete di Istituto avvenga sempre e solamente sotto la propria supervisione e unicamente con gli strumenti messi a disposizione dalla scuola;

c) dare chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc.), condividendo con gli alunni la netiquette e vigilando sul rispetto della stessa;

d) assumersi la responsabilità della tracciabilità dell'utilizzo e del mantenimento in buono stato della strumentazione tecnologica da lui stesso e dagli alunni utilizzata, segnalando prontamente eventuali malfunzionamenti o danneggiamenti al tecnico informatico;

e) non divulgare le credenziali di accesso agli account (username e password) e/o, nel caso ne sia a conoscenza, alla rete wifi;

f) nel caso si sia effettuato l'accesso al proprio account dalla postazione di classe, non allontanarsi dalla eventuale postazione di lavoro, lasciandola incustodita, se non prima di aver effettuato la disconnessione;

g) non salvare sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili;

h) proporre agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento (creati per la didattica, istituzionali e/o preventivamente verificati dall'insegnante stesso).

3.2 Utilizzo delle postazioni informatiche da parte degli studenti

Gli studenti possono utilizzare tutte le apparecchiature informatiche di cui l'IISS "MAJORANA - GIORGI" di Genova dispone, sotto la guida e vigilanza dei docenti referenti ed in conformità con il progetto educativo, nel rispetto del seguente regolamento. Per gli studenti sono resi disponibili:

- piattaforme ad accesso riservato con la possibilità di scaricare e caricare compiti, materiali didattici, lezioni e comunicare con i docenti della propria classe;
- il sito ufficiale della scuola dal quale è possibile visualizzare varie sezioni tra cui l'Albo d'Istituto e l'informativa relativa all'anno scolastico in corso, cui può accedere qualunque utente della rete compresi i genitori.

Gli alunni imparano a:

- conoscere l'origine delle informazioni a cui si accede o che si ricevono;
- utilizzare fonti alternative di informazione per proposte comparate;
- ricercare il nome dell'autore, la data dell'ultimo aggiornamento del materiale e possibili altri link;
- rispettare i diritti d'autore e i diritti di proprietà intellettuale;
- usare i motori di ricerca;
- essere coscienti dei rischi a cui si espongono quando sono in rete.

Devono essere educati a riconoscere e ad evitare gli aspetti negativi di Internet (siti che inneggiano alla violenza, il razzismo e lo sfruttamento dei minori).

3.3 Regole generali

L'utilizzo da parte degli studenti delle apparecchiature elettroniche ed informatiche sia nei lavori di gruppo che negli interventi individuali avviene nel rispetto delle seguenti regole:
a) utilizzare le apparecchiature informatiche nonché l'accesso in rete, sempre sotto la supervisione del docente. Costituiscono eccezione i casi di comprovata necessità (situazioni di handicap, certificazione dsa) per i quali è possibile l'utilizzo a scuola del PC personale dell'alunno, previa autorizzazione del Dirigente Scolastico;
b) accedere all'ambiente di lavoro con il corretto account, non divulgandone le credenziali di accesso (username, password), e archiviare i propri documenti in maniera ordinata e facilmente rintracciabile nella cartella personale presente nel Server della didattica o su supporto esterno;
c) in caso di riscontro di malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate comunicarlo immediatamente all'insegnante;
d) non eseguire tentativi di modifica della configurazione di sistema delle macchine;
e) accedere alla rete solo in presenza o con l'autorizzazione dell'insegnante responsabile dell'attività;
f) non utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);
g) chiudere correttamente la propria sessione di lavoro.

3.4 Regole specifiche

In particolare modo gli studenti, al fine di favorire l'integrazione e l'accesso alle tecnologie informatiche anche ai compagni meno preparati, sono tenuti al rispetto delle seguenti buone passi (lotta al cyberbullismo):
a) rispettare le persone diverse per nazionalità, cultura, religione, sesso: il razzismo e ogni tipo di discriminazione sociale non sono ammessi;
b) non essere intolleranti con chi ha scarsa dimestichezza con le tecnologie informatiche o commette errori concettuali;
c) non rivelare dettagli o informazioni personali o di altre persone (indirizzi, numeri di telefono);
d) richiedere sempre il permesso ai genitori in caso di minori, prima di iscriversi a qualche mailing-list o sito web che lo richieda;
e) non dare indirizzo e numero di telefono a persone incontrate sul web, in caso di minori, senza chiedere il permesso ai genitori (questo perché non si può avere la certezza dell'identità della persona con la quale si sta comunicando);
f) non prendere appuntamenti con le persone conosciute tramite web, in caso di minori, senza aver interpellato prima i genitori;
g) non inviare foto, filmati, o altro materiale riconducibile alla propria persona senza aver chiesto, in caso di minori, preventivamente il consenso dei propri genitori;
h) non inviare foto, filmati, o altro materiale riconducibile ad altre persone senza avere prima richiesto il consenso del diretto interessato, ovvero nel caso di minori il consenso dei rispettivi genitori;
h) riferire sempre a insegnanti e genitori se si è raggiunti in internet da immagini o scritti che infastidiscono;
i) se qualche studente dovesse venire a conoscenza che altri compagni non rispettano le suddette regole è opportuno parlane con gli insegnanti e con i genitori;
l) chiedere il permesso ai genitori, nell'ipotesi di minori che utilizzino postazioni internet nelle proprie abitazioni, ovvero agli insegnanti, nell'ipotesi di apparecchiature scolastiche, prima di scaricare dal web materiale di vario tipo.

3.5 Utilizzo delle postazioni da parte del personale ATA

a) Il personale ATA deve aver cura della propria postazione pc o delle eventuali postazioni alle quali ha accesso, rispettare il presente regolamento facendo particolare attenzione alle seguenti disposizioni:
b) utilizzare la postazione e il collegamento a internet solo per finalità di servizio;
c) evitare di lasciare le e-mail o file personali sui computer o sul server della scuola;
d) effettuare periodicamente il backup dei dati relativi alle applicazioni in uso
e) ricordare di chiudere la connessione (e di spegnere il computer) alla fine della sessione di lavoro su Internet e disabilitare la navigazione su Internet del laboratorio (qualora sia stata attivata);
f) comunicare tempestivamente al responsabile indicato dal DS malfunzionamenti e anomalie
g) non collegare alla rete e ai PC dispositivi propri e diversi da quelli in dotazione dell'Istituzione scolastica

Art. 4 Password e account d'ingresso alla rete

Le password di accesso alla rete nonché ai vari programmi in rete, sono attribuite dal Dirigente Scolastico, che si avvale della collaborazione di personale appositamente incaricato. L'utente che riceve le credenziali è tenuto a:
a) conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione;
b) scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima;
c) non 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;
d) chiedere la sostituzione della password nel caso si sospetti che la stessa abbia perso la segretezza.

Art. 5 Posta elettronica

La casella di posta elettronica gestita da postazioni presenti nell'Istituto, è uno strumento legato alla finalità dell'insegnamento e alle attività ad esso connesse. Il personale della scuola titolare di casella di posta elettronica è responsabile del corretto utilizzo della stessa (art.615 comma 5 e segg. c.p.). L'utilizzo della casella deve avvenire nel rispetto delle seguenti buone prassi:
a) non aprire messaggi insoliti o provenienti da sconosciuti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli. Anche i messaggi provenienti da conosciuti possono contenere file eseguibili (quindi virus), pertanto bisogna fare attenzione alle estensioni, es. exe., escr, pif.,bat., cmd., questi ultimi non devono essere aperti se non conosciuta la provenienza;
b) bloccare messaggi che diffondono "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata), possono limitare l'efficienza del sistema postale;
c) utilizzare formato compresso nell'ipotesi di invio di file pesanti, a titolo di esempio *.zip *.rar *.jpg; d) per l'invio di file ad altre istituzioni pubbliche o private è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf);
e) prima di iscriversi a "mailing list" esterne bisogna verificare in anticipo se il sito sia affidabile;
f) cancellare dalla casella i documenti ritenuti inutili al fine di evitare l'occupazione di spazio di memoria.

art.6 Antivirus

Il personale che accede alle postazioni informatiche della scuola deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'ITIS mediante virus o mediante ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc..). A tal fine il personale è tenuto:
a) a controllare la presenza e il regolare funzionamento del software antivirus della scuola. Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto al responsabile;
b) ogni dispositivo magnetico di provenienza esterna alla scuola dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovrà essere utilizzato.

Art.7 Sito web dell'Istituto

La responsabilità e la gestione del sito web dell'Istituto è del rappresentante legale, ovvero del Dirigente Scolastico. La gestione del sito può essere affidata dal Dirigente Scolastico ad un docente dell'Istituto. Nell'ipotesi di assenza di docenti con le competenze tecniche necessarie per la gestione del sito il Dirigente Scolastico potrà affidare, conservando ogni responsabilità in qualità di rappresentane legale, ad un soggetto esterno. Il sito web dell'IISS "MAJORANA - GIORGI" di Genova (www.majorana.gov.it) si pone come strumento informativo interno ed esterno, di comunicazione di contenuti educativi e di attività didattico-formative. L'istituto detiene i diritti d'autore dei documenti prodotti in proprio o dei quali è stato chiesto e ottenuto il permesso di pubblicazione. Nella pubblicazione di immagini degli alunni minorenni è necessaria la preventiva liberatoria da parte dei genitori. Anche in presenza di liberatoria, l'Istituto procede con la

massima attenzione, preferendo pubblicare immagini a campo lungo, senza primi piani; immagini di gruppo in attività piuttosto che di singoli. Il sito rispetta i requisiti di accessibilità per i disabili di cui alla L.9/1/2004. Nel sito dell'Istituto sono presenti tutte le informazioni relative all'organizzazione della scuola pertanto il personale, studenti e genitori sono obbligati a consultare il sito in aggiunta e/o sostituzione delle comunicazioni fornite nelle forme tradizionali.

Art.8 Informativa e trattamento dei dati

9.1 Generalità

Informativa e trattamento dei dati personali ai sensi dell'art. 13 del d.l. 30/06/2003 n.196 Ai sensi di quanto previsto dalla normativa vigente questo Istituto è titolare del trattamento dei dati personali. Le finalità e modalità del trattamento dei dati sono:

a) il trattamento viene effettuato ad opera di soggetti appositamente incaricati, che si avvarranno di strumenti elettronici e non, configurati in modo da garantire la riservatezza dei dati e nel rispetto del segreto professionale;

b) i dati potranno essere utilizzati per circolari e corrispondenza nell'ambito dell'attività istituzionale dell'Istituto;

c) il trattamento cessa nel momento in cui termina la permanenza dello studente a scuola, salvo il caso dei CV degli studenti diplomati, oggetto di specifica normativa dedicata;

d) il trattamento dei dati è obbligatorio per legge quando è indispensabile per adempiere alle finalità istituzionali della scuola;

e) le conseguenze di un esplicito rifiuto al trattamento comporteranno l'impossibilità da parte della scuola di impiegare il registro elettronico;

f) i dati personali non saranno oggetto di diffusione e saranno a conoscenza solo del personale responsabile e incaricato al trattamento

9.2 Informativa e trattamento dei dati personali ai sensi dell'art. 7 del d.l. 30/06/2003 n.196.

L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile. L'interessato ha diritto di ottenere l'indicazione:

a) dell'origine dei dati personali;

b) delle finalità e modalità del trattamento;

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

9.3 L'interessato ha diritto di ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

9.4 L'interessato ha diritto di opporsi, in tutto o in parte, per motivi legittimi:

a) al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.