ISTITUTO COMPRENSIVO PRIMO MILAZZO

Via Del Quartiere, 26 – 98057 Milazzo (ME) Tel.: 090 9281409 – Fax: 090 9241399
E-Mail: meic88300c@istruzione.it – meic88300c@pec.istruzione.it
C.F. 82002420832 - Cod. Mecc.: MEIC88300C

Al prof. Alfonso Alessi
Ai responsabili di plesso
Ai docenti
Al DSGA
Fascicolo personale
Sito WEB
Amministrazione Trasparente
Argo scuola Next

I.C PRIMO - MILAZZO
Prot. 0011339 del 13/10/2021
07 (Uscita)

Oggetto: Incarico Responsabile laboratori e Nuove Tecnologie Scuola secondaria - Anno scolastico 2021/2022.

IL DIRIGENTE SCOLASTICO

Visto	il Piano di Miglioramento della scuola;
Visto	il PTOF triennale approvato dagli Organi Collegiali;
Visto	Il Piano annuale delle attività approvato dal Collegio dei Docenti;
Visto	l'art. 25 del dlgs n. 165 che dispone che sia il Dirigente Scolastico ad adottare i provvedimenti di gestione del personale
Visto	il C.C.N.L. del comparto scuola attualmente vigente;
Visto	il contratto integrativo di istituto con il quale sono state ripartite le somme destinate alla retribuzione dei docenti impegnati nei progetti di ampliamento dell'offerta formativa;
Considerato	**Che il professore Alfonso Alessi ha adeguate competenze ed esperienza nello specifico settore;**
Vista	la disponibilità del docente;
Considerato	la necessaria copertura finanziaria delle spese conseguenti il presente conferimento di incarico per attività aggiuntive
Acquisito	Il parere del DSGA;
Considerata	la necessità di garantire la piena funzionalità delle LIM, delle attrezzature multimediali e dei laboratori anche nell'eventualità di attivazione della DAD o della DID
Considerato	che, pertanto, si rende necessario procedere alla formalizzazione degli incarichi.
Vista	**la coerenza con le priorità e gli obiettivi di processo (PDM/PTOF)**
Vista	La normativa vigente;

NOMINA

Il professore **Alfonso Alessi** responsabile delle tecnologie digitali e laboratori di informatica per la scuola Secondaria a.s. **2021/2022.**

Il professore per la parte relativa alla tutela della privacy e all'uso corretto da parte degli alunni di internet, si raccorderà con il responsabile della protezione dei dati personali, ing. Fabio Genovese. Al fine di adeguare le strumentazioni tecnologiche compresi i programmi, ecc. d'intesa con l'ing. Genovese è invitato presentare una proposta di adeguamento della struttura di rete e delle tecnologie digitali, proponendo le necessarie misure da garantire anche con eventuali acquisti di strumentazione e programmi di adeguamento.

I docenti interessati che richiedano la supervisione del prof. Alessi, dovranno presentare apposita richiesta scritta con descrizione del tipo di problema evidenziato.

Pertanto, al fine di monitorare gli interventi, il giusto utilizzo da parte dei docenti delle strumentazioni tecnologiche nonché la responsabilizzazione degli stessi, il professore è invitato a compilare, di volta in volta un verbale di descrizione del tipo di intervento (sottoscritto dai docenti) per cui richiedere il preventivo e il conseguente affidamento ad una ditta specializzata.

Il professore provvederà alla custodia e alla cura del materiale del laboratorio, verificandone l'uso, la manutenzione e le caratteristiche di sicurezza, intervenendo con proposte nelle procedure di acquisto per il rinnovo della strumentazione. In particolare provvede a :

- controllare che siano presenti le istruzioni sulle norme di comportamento nell'uso delle strumentazioni e in caso di emergenze- controllare che le apparecchiature in uso o da acquistare abbiano, su di una etichetta verde o sulla targhetta delle caratteristiche, il marchio IMQ, al fine di garantire la rispondenza alle norme di sicurezza;
- segnalare al Responsabile del Servizio di Prevenzione e Protezione eventuali carenze del laboratorio e degli strumenti in esso utilizzati che possano causare pericolo alla sicurezza delle operazioni.
- Effettuare controlli periodici per verificare eventuali situazioni di disfunzioni
- Segnalare la necessità' di eventuali manutenzioni, integrazioni, adeguamento e incremento delle dotazioni.
- Predisporre le proposte per eventuali nuovi acquisti e controllo materiale acquistato .Effettuare la verifica della funzionalità dei materiali e delle attrezzature assegnate, segnalando l'eventuale esigenza di reintegro di materiali di consumo e di ripristino delle condizioni ottimali di utilizzo delle attrezzature danneggiate.
- Attuare un controllo a fine anno scolastico e predisporre una relazione scritta sulle rilevazioni compiute, sullo stato dei beni del laboratorio compilando apposito modulo in cui vengono indicati: beni deteriorati da scaricare, beni da riparare, beni scomparsi e per quali presunte ragioni.
- Segnalare tempestivamente al dirigente scolastico emergenze e problemi riscontrati, al fine di implementare un efficiente utilizzo del laboratorio.
- Supporto tecnico-didattico al personale docente.
- Fornire agli utilizzatori informazioni inerenti il corretto uso e le misure di sicurezza applicabili al posto di lavoro, le modalità di svolgimento dell'attività didattica e l'uso dei DPI quando presenti.
- effettuare il collaudo delle nuove tecnologie, insieme con il docente coordinatore di materia e firmare il relativo verbale
- verificare annualmente l'obsolescenza delle attrezzature in dotazione al laboratorio e predisporre la relazione di scarico inventariale, da consegnare al Referente per l'inventario
- supporto ai docenti in caso di DAD o DID

Fino al perdurare dell'emergenza COVID 19, in considerazione del fatto che alcuni laboratori sono utilizzati come aule didattiche, il responsabile curera' comunque la parte relativa alla strumentazione, alla manutenzione ed al buon funzionamento delle dotazioni di laboratorio, delle LIM e delle attrezzature multimediali.

Il compenso, che sarà stabilito in sede di contrattazione, sarà erogato attraverso il cedolino unico a cura del Service Personale Tesoro (SPT) e sarà corrisposto dopo la presentazione di una relazione finale sulle attività effettivamente svolte e il monitoraggio del controllo del processo organizzativo.

IL DIRIGENTE SCOLASTICO
Dott.ssa Elvira Rigoli
Firma autografa sostituita a mezzo stampa
ai sensi dell'ART 3 CO. 2 del D. Lgs. N. 39/1993

ISTITUTO COMPRENSIVO PRIMO MILAZZO

E-Policy - Misure minime di sicurezza informatica/uso consapevole T.I.C.

Premessa

Uno dei punti di forza del nostro istituto è rappresentato dalle dotazioni tecnologiche informatiche: laboratori, Lim, tablet, computer nelle aule per i collegamenti interni ed esterni, computer in rete per il lavoro degli uffici amministrativi .
L'utilizzo di internet nelle classi e nei laboratori, le classi virtuali, il lavoro in rete presentano potenzialmente dei rischi per cui si ritiene necessario prevenire e/o ridurre i rischi per un uso improprio, regolamentando l'utilizzo delle nuove tecnologie informatiche, nel rispetto delle direttive di settore del MIUR.
In questo documento sono definite:

- le norme relative all'accesso alle postazioni in rete della scuola da parte dei diversi soggetti operanti nell'Istituto (docenti, ATA, studenti, eventuali soggetti esterni alla scuola);
- le norme riguardanti l'accesso ai servizi resi disponibili sui computer in rete da parte dei diversi soggetti operanti nell'Istituto;
- le regole riguardanti le garanzie a tutela della privacy nell'uso degli strumenti tecnologici d'Istituto.

Vengono individuati anche gli strumenti hardware e/o software da impiegare per evitare o ridurre al minimo: l'uso improprio dell'accesso a Internet (con particolare riguardo alla gestione relativa al traffico generato sulla LAN in uscita e in entrata verso Internet); i danni causati da virus o da software; i tempi di recupero della piena funzionalità dell'infrastruttura, in caso di crash di sistema.

* * *

Articolo 1) -Internet a scuola

1. L'utilizzo della rete interna/esterna (web) deve avvenire all'interno della programmazione didattica e nell'ambito delle esigenze relative agli uffici amministrativi, attraverso un utilizzo mirato e consapevole che può garantire la "sicurezza informatica".
2. La scuola favorisce una "alfabetizzazione informatica" in modo che per tutti, Internet possa essere un diritto ed una risorsa. Il docente è il primo soggetto che favorisce l'uso corretto della rete, guidando gli studenti nelle attività online, stabilendo obiettivi chiari di ricerca, insegnando le strategie appropriate nella definizione e gestione della risorsa informatica.
3. L'Istituto regolamenta l'uso dei laboratori indicando norme che consentono di vigilare sull'uso corretto dell'accesso ad Internet.
4. Da quest'anno scolastico, sarà predisposto l'uso in classe dei "Tablet" su richiesta del Docente, per poter fornire un ulteriore strumento multimediale allo svolgimento della didattica.

Articolo 2) -Le strategie attuate dalla scuola per garantire la sicurezza delle TIC

1. Le strategie attuate dalla scuola per garantire la sicurezza delle Tecnologie dell'Informazione e della Comunicazione (TIC) sono le seguenti:

- il Dirigente Scolastico si riserva, sentiti i responsabili, di limitare l'accesso e l'uso della rete interna ed esterna (web), secondo i normali canali di protezione presenti nei sistemi operativi e utilizzando, se necessario, software aggiuntivi come Firewall;
- la Scuola promuove e adotta ogni accorgimento per evitare comportamenti contrari alle norme del presente regolamento, quali:
  - scaricare file video-musicali protetti da copyright;
  - visitare siti non necessari ad una normale attività didattica;
  - alterare i parametri di protezione dei computer in uso;
  - utilizzare la rete per interessi privati e personali che esulano dalla didattica;
  - non rispettare le leggi sui diritti d'autore;
  - navigare su siti non accettati dalla protezione interna alla scuola.

2. Tutti gli utenti dei servizi devono essere consapevoli che:

- il sistema informatico è periodicamente controllato dai responsabili;
- la scuola controlla periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni dispositivo;
- è vietato salvare o scaricare da Internet software non autorizzati;
- al termine di ogni collegamento la connessione deve essere chiusa;
- i responsabili si occupano dell'aggiornamento periodico degli antivirus sulle macchine;
- l'utilizzo di CD, chiavi USB personali e di altri strumenti esterni di archiviazione dati deve essere previamente autorizzato e sottoposto a controllo antivirus;
- la scuola si riserva di limitare il numero di siti visitabili e le operazioni di download;

- il materiale didattico dei docenti può essere messo in rete, anche su siti personali collegati all'Istituto, sempre nell'ambito del presente regolamento e nel rispetto delle leggi.

Articolo 3)-Accertamento dei rischi e valutazione dei contenuti di Internet

USO DI INTERNET

- **Si ricorda che la navigazione in Internet non è libera**, ma progettata, guidata e seguita dall'insegnante. **Si può accedere ad internet solo previa autorizzazione del proprio insegnante e dopo che lo stesso avrà fornito il percorso di navigazione. La navigazione libera è vietata.**
- Qualora il docente ritenga utile per la didattica l'accesso ad internet da parte di uno o più alunni, il percorso in rete deve essere fornito e sorvegliato dal docente, così come i risultati della ricerca e i contenuti trovati dovranno essere monitorati dall'insegnante responsabile del lavoro.

1. L'Istituto utilizza la connettività Wodafone, senza l'uso di ulteriori Firewall di controllo del " traffico Internet ". Essendo l'uso di Firewall supplementari fortemente limitante per la velocità di connessione, saranno eseguite verifiche a campione, per verificare la correttezza nell'uso delle macchine.
2.Tutti gli utilizzatori devono essere pienamente coscienti dei rischi cui si espongono collegandosi alla rete, riconoscendo ed evitando gli aspetti negativi (pornografia, violenza, razzismo …).
3. Gli utilizzatori rispondono personalmente di qualsiasi uso improprio e/o di eventuale materiale non idoneo e/o per eventuali conseguenze causate dall'accesso al Web.

Articolo 4)-Reati e violazioni della legge

1. Sono vietati tutti i comportamenti (apparentemente innocui) che presuppongono dei veri e propri reati informatici, quali:
   - Accesso abusivo ad un sistema informatico e telematico
   - Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico
   - Danneggiamento informatico
   - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
   - Frode informatica
   - Ingiuria
   - Diffamazione
   - Minacce e molestie.
2. L'Istituto, al fine di prevenire condotte inappropriate degli utenti, potenzialmente riconducibili ai reati di cui sopra, stabilisce alcune norme essenziali da rispettare e comportamenti corretti da tenere.
3. L'Istituto, in ogni caso, non sarà responsabile per le condotte illecite poste deliberatamente in essere dagli utenti del servizio.

Articolo 5)-Utilizzo dei servizi Internet (e-mail, chat, forum, download)

1. L'insegnante di classe che ha nella propria programmazione l'utilizzo di Internet è responsabile di quanto avviene nelle proprie ore di laboratorio.
2. L'invio e la ricezione di e-mail e allegati è soggetto ad autorizzazione. E' vietato utilizzare e-mail personali ad uso privato.
3. E' vietata la pratica delle chat-line.
4. Gli studenti non possono usare i computer in rete senza il coordinamento del docente.
5. E' vietato il download a fini personali di file musicali, foto, software, video, ecc., tranne nel caso di specifiche attività didattiche preventivamente programmate.
6. Il mancato rispetto da parte degli studenti delle norme così definite comporterà l'irrogazione di sanzioni disciplinari.

Articolo 6)-Sicurezza della rete interna (LAN)

1. L'Istituto dispone di rete LAN dedicata, in parte cablata e wi-fi, che copre tutti i locali della Scuola.
2. Il collegamento di computer portatili o palmari personali alla rete di Istituto deve essere autorizzato.
3. L'accesso alla rete Wifi, è concessa esclusivamente per un uso didattico, pertanto il docente può chiedere l'abilitazione all'uso della rete scolastica su una sola macchina personale (Notebook o Tablet), la quale verrà configurata dal responsabile dei Labopratori. Per nessun motivo la chiave di criptazione potrà essere messa a disposizione di Docenti, Personale o Alunni.

Articolo 7) -Linee guida per gli Studenti

1. Gli Studenti devono attenersi alle seguenti indicazioni:

- non utilizzare giochi né in locale, né in rete;
- salvare sempre i lavori propri (file) in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarebbe preferibile utilizzare una PENDRIVE esclusivamente per i file scolastici, dove poter salvare i propri lavori. 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;
- mantenere segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della scuola;
- non inviare a nessuno fotografie personali o di propri amici;
- chiedere sempre al Docente il permesso di scaricare documenti da Internet;
- chiedere sempre l'autorizzazione al Docente prima di iscriversi a qualche concorso o prima di riferire l'indirizzo della propria scuola;

- riferire immediatamente al Docente nel caso in cui qualcuno invii immagini inappropriate od offensive. Non rispondere, in ogni caso, al predetto invio;
- riferire all'insegnate in caso di reperimento di immagini inappropriate od offensive durante la navigazione su Internet;
- riferire al Docente, o comunque ad un adulto, qualora qualcuno su Internet chieda un incontro di persona;
- ricordarsi che le persone che si "incontrano" nella Rete sono degli estranei e non sempre sono quello che dicono di essere;
- non è consigliabile inviare mail personali, perciò rivolgersi sempre all'insegnante prima di inviare messaggi di classe;
- non caricare o copiare materiale da Internet senza il permesso dell'insegnante o del responsabile di laboratorio.

Articolo 8) -Linee guida per Docenti e personale ATA

1. I Docenti ed il personale ATA devono attenersi alle seguenti indicazioni:

- evitare di lasciare le e-mail o file personali sui computer o sul server della scuola;
- 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;
- discutere con gli alunni delle norme adottate dalla scuola e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet;
- dare chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informare gli Studenti che le navigazioni sono monitorate;
- 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);
- ricordare agli alunni che qualsiasi uso improprio di internet e/o l'utilizzo di materiale non idoneo, comporta l'irrogazione di sanzioni disciplinari;
- tutti gli utilizzatori di computer, siano essi docenti, personale ATA e studenti, non devono lasciare a lungo sui computer in uso, file di grosse dimensioni e/o non più utilizzati per molto tempo onde evitare di occupare spazio.

Articolo 9) –Sanzioni

1. A fronte di violazioni accertate delle regole stabilite dal presente regolamento, l'Istituto, su valutazione del responsabile di laboratorio e del Dirigente Scolastico, si assume il diritto di impedire l'accesso dell'utente a Internet per un certo periodo di tempo, rapportato alla gravità.
2. 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. Rimangono comunque applicabili ulteriori sanzioni disciplinari, eventuali azioni civili per danni, nonché l'eventuale denuncia del reato all'Autorità Giudiziaria.
3. 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.

Articolo 10) -Informazione sull'uso corretto delle TIC della scuola

1. Le regole di base relative all'accesso ad Internet sono parte integrante del regolamento d'Istituto, e sono esposte all'albo dell'Istituto, all'interno dei laboratori di informatica e negli uffici amministrativi.
2. Tutto il personale scolastico (docente ed ATA) analizzerà queste indicazioni e le sottoscriverà all'inizio dell'anno scolastico, all'inizio del rapporto di lavoro ed ogni qualvolta vi sarà apportata una variazione e sarà coinvolto nel suo ulteriore sviluppo, sempre tenendo conto che l'uso della rete sarà sottoposto a monitoraggio.
3. Sarà cura del Docente responsabile del laboratorio e dei vari Docenti utenti del medesimo illustrare didatticamente i contenuti delle norme per l'utilizzo delle TIC agli Studenti, tenendo conto della loro età ed evidenziando le opportunità ed i rischi connessi all'uso della comunicazione tecnologica.
4. I genitori saranno informati sull'uso accettabile e responsabile di Internet nella scuola e su alcuni consigli da seguire a casa, anche tramite l'esposizione del seguente regolamento all'albo, la sua pubblicazione sul sito web della scuola e l'eventuale sua consultazione, in cartaceo, in segreteria. All'atto dell'iscrizione o all'inizio dell'anno scolastico la scuola chiede ai genitori degli studenti minori di 18 anni di età il consenso all'uso di Internet per il loro figlio e per la pubblicazione dei suoi lavori e della sue fotografie.

Articolo 11) -Sito web della scuola e servizi on-line alle famiglie, studenti, docenti/utenti esterni

1. Sarà cura del responsabile (webmaster) la gestione delle pagine del sito della scuola, nonché la garanzia che il contenuto sul sito sia accurato ed appropriato.
2. Per i documenti che si trovano sul sito viene chiesto ed ottenuto il permesso dall'autore proprietario. Le informazioni pubblicate sul sito della scuola relative alle persone da contattare rispetteranno le norme vigenti sulla privacy.
3. 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.
4. 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.

5. 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.

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

Articolo 12) -Altre forme tecnologiche di comunicazione.

1. E' vietato l'utilizzo in classe e nei locali della scuola dei cellulari e altri dispositivi mobili, tranne quelli per uso didattico, preventivamente autorizzati dal dirigente scolastico e dal responsabile di laboratorio.

Articolo 12) -Diritti d'Autore

1. La legge 159/93 dispone, all'art. 1, che chiunque abusivamente riproduce a fini di lucro, con qualsiasi procedimento, la composizione grafica di opere o parti di opere letterarie, drammatiche, scientifiche, didattiche e musicali, che siano protette dalla legge ovvero, pone in commercio, detiene per la vendita o introduce a fini di lucro le copie, viola i diritti d'autore.
2. Esempi di questo tipo di violazioni si possono verificare: quando una copia non autorizzata di un'opera digitale è caricata su un server e messa a disposizione degli utenti; quando l'utente ottiene il documento, il software o il brano mp3 messo a disposizione in rete o acquistato e ne fa un uso illegittimo; quando si opera la duplicazione abusiva di software proprietario a scopo di lucro o per un semplice fine di risparmio personale.
3. Qualora nel realizzare lavori didattici o pagine web, si inseriscono, a scopo di discussione, di critica o di informazione culturale, parti di opere, brevi estratti o citazioni (mai l'opera integrale) si dovrà menzionare chiaramente il nome dell'autore e la fonte, per evitare infrazioni di copyright.

Articolo 13) -Laboratori didattici

1. I laboratori sono dotati di materiale inventariato come hardware, software, manuali-testi da utilizzare per scopi didattici.
2. I docenti possono richiedere in prestito per scopi esclusivamente didattici (consultazione, ricerche, prove) le dotazioni, previa registrazione su apposito registro.
3. I docenti, gli alunni e tutto il personale scolastico avranno massima cura delle attrezzature e delle dotazioni utilizzate. Ogni spostamento di materiali, macchine o parti di esse (es. mouse, tastiere, monitor, ecc.) da un laboratorio all'altro deve essere autorizzato.
4. **È vietato utilizzare programmi (software) non autorizzati o dei quali l'Istituto non possieda licenza d'uso. I programmi sui supporti originali sono custoditi in un luogo sicuro dell'Istituto. Per l'installazione, il ripristino o la configurazione, il personale tecnico addetto si avvarrà della copia (consentita dalla legge per questo uso).**
5. **È vietata la diffusione di programmi (software) o copie di esso con licenza rilasciata all'Istituto.**
6. **È vietato l'uso di floppy disk, CD ROM, CD R/RW, DVD, memorie e dispositivi USB personali se non consentiti dall'insegnante, previo controllo con software antivirus.**
7. L'Istituto promuove al suo interno l'uso del software non proprietario (open source) come da indicazioni ministeriali.
8. L'installazione dei programmi o l'operatività ed affidabilità delle attrezzature è di competenza degli insegnanti e del personale assistente tecnico.
9. **È vietato a chiunque non sia autorizzato installare programmi, modificare installazioni di programmi e di rete, cambiare le configurazioni delle macchine.**
10. L'assistenza per piccoli interventi è assicurata dal personale aiutante tecnico disponibile.
11. Il personale tecnico svolge le proprie mansioni di collaborazione e assistenza nei laboratori al fine di garantire l'efficienza dei locali e delle attrezzature e lo svolgimento regolare delle attività didattiche.
12. Per i laboratori della scuola, viene individuato il responsabile che sovraintende al corretto funzionamento delle macchine, accerta e segnala le eventuali anomalie, ecc.
13. Il docente che accompagna gli alunni nei laboratori, dovrà assicurarsi dell'accensione e del corretto funzionamento delle macchine ed alla fine della lezione, accerterà che le apparecchiature siano funzionanti, provvedendo al contempo a spegnerle così come l'interruttore generale e che l'aula sia lasciata in condizione adeguata per ricevere un'altra classe.
13. Chiunque utilizzi dispositivi e ne verifica il malfunzionamento deve segnalare tempestivamente al responsabile del laboratorio, al DSGA e al dirigente scolastico, i quali interverranno o annoteranno l'anomalia e provvederanno alla risoluzione del problema.
14. Per guasti che richiedono l'intervento dell'assistenza tecnica esterna, il personale richiederà per iscritto l'intervento delle ditte incaricate, spegnendo gli interruttori e lasciando l'attrezzatura in questione inattiva, apponendo il cartello di "fuori servizio".
15. È vietato alle persone non autorizzate manomettere o intervenire sulle apparecchiature o impianti di qualsiasi natura, installare accessori che pregiudichino la sicurezza delle persone o che rischino di causare danni all'apparecchiatura stessa.
16. 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 CO_2.
17. Il docente presente, se possibile, staccherà l'interruttore generale del laboratorio. Per le procedure dettagliate, al riguardo, si rinvia al "Piano di Emergenza" predisposto.
18. Nei laboratori deve essere sempre presente apposita segnaletica di sicurezza relativa sia ai rischi specifici, sia alla gestione delle emergenze.
19. È obbligatorio consultare comunque le procedure specifiche disponibili nei singoli laboratori.
20.Nei laboratori di didattica non devono essere trattati né conservati dati sensibili o giudiziari.
Non sono permessi server amministrativi o server Internet in questa rete.
Nell'implementazione delle politiche di sicurezza sul firewall per le reti didattiche è necessario tenere traccia di ogni connessione e dell'accesso degli utenti alla rete.

Allegato 1: Regolamento interno ai laboratori didattici informatici

I laboratori dell'Istituto sono patrimonio comune. Pertanto il rispetto e la tutela delle attrezzature sono condizioni indispensabili per il loro utilizzo e per garantirne l'efficienza. I laboratori informatici e le tecnologie didattiche informatiche e multimediali sono a disposizione di tutti i docenti e studenti dell'Istituto. Gli utilizzatori devono attenersi al seguente regolamento interno:

1. Per ogni Laboratorio viene nominato **un Responsabile(sub-consegnatario**), garante della conservazione, della tutela di tutti i beni mobili in carico al Laboratorio e del rispetto del presente Regolamento.
2. L'accesso degli alunni e docenti al laboratorio è regolato secondo l'orario delle lezioni, dando priorità alle classi che lo hanno prenotato. È vietato l'uso dei laboratori e di Internet per scopi personali finanziari, pubblicitari, politici e per gioco. L'uso dei laboratori e delle attrezzature per attività di altra natura deve essere autorizzato.
3. Nel Laboratorio le classi o gruppi di alunni entrano secondo l'orario didattico in vigore per l'anno scolastico in corso; detto orario viene esposto all'esterno della porta di ingresso. L'utilizzo non previsto del laboratorio deve essere concordato con il responsabile del laboratorio e, comunque, deve essere giustificato da ragioni didattiche. In assenza duratura del Responsabile, il permesso va richiesto direttamente al Dirigente Scolastico.
4. **La responsabilità sulla custodia ed il corretto uso delle attrezzature viene trasferita automaticamente dal Responsabile di Laboratorio all'Insegnante momentaneamente presente con o senza la propria classe o gruppo di allievi.**
5. Il Responsabile di Laboratorio può operare nello stesso in tutte le ore libere.
6. Gli altri Insegnanti operanti nel Laboratorio possono programmare presenze extra orario in funzione della preparazione delle lezioni
7. I progetti che prevedono l'uso del laboratorio devono essere preventivamente segnalati al responsabile dei servizi informatici.
8. Le classi possono accedere in laboratorio solo in presenza del docente, che è tenuto a vigilare sugli alunni e a svolgere l'attività didattica programmata. Si entra in laboratorio solo dopo l'uscita della classe dell'ora precedente.
9. È proibito portare e consumare cibi o bevande nei laboratori.
10. Gli alunni portano nei laboratori soltanto il materiale necessario per lo svolgimento della lezione.
11. Per l'uscita dal laboratorio in caso di emergenza ci si deve attenere alle disposizioni date ed illustrate in ogni locale dell'edificio e portarsi nel luogo di ritrovo indicato, interrompendo immediatamente ogni attività, incolonnandosi con calma.
12. Al termine dell'attività il docente si accerta della situazione del materiale (attrezzature, accessori, ecc.) e di eventuali anomalie o mancanze; verifica inoltre che siano spente tutte le apparecchiature; l'aula sia lasciata in condizione adeguata per ricevere un'altra classe; l'uscita degli alunni dal laboratorio avvenga ordinatamente.
13. L'insegnante segnala i problemi riscontrati sulle macchine, i guasti e gli eventuali danni riscontrati sulle postazioni o sugli arredi (scritte, etc).
14. Ogni alunno è responsabile della postazione usata durante l'ora di lezione ed è tenuto a segnalare immediatamente all'insegnante o alla vice preside qualsiasi guasto o disfunzione riscontrata oltre che la presenza di scritte rilevate sulla postazione stessa. *Atti di vandalismo o di sabotaggio verranno perseguiti nelle forme previste, compreso il risarcimento degli eventuali danni arrecati.*
15. Gli alunni, prima di uscire dal laboratorio, avranno cura di risistemare le sedie e gettare negli appositi contenitori eventuali rifiuti; i PC dovranno essere lasciati disconnessi enspenti.
16. non è consentito modificare a qualsiasi titolo le impostazioni dei computer. Non cercare di modificare le impostazioni (salvaschermo, sfondo, colori, risoluzioni, suoni, pagina iniziale di Internet, account di posta elettronica...). I menu di Office non devono subire variazioni: devono restare attive le barre dei menu standard e di formattazione. La posizione delle icone deve rimanere invariata.
17. E' consentito memorizzare temporaneamente i propri file nella cartella Documenti, creando una cartella nella quale memorizzare i dati *es. classe 1 A.* I file non archiviati secondo questo criterio potranno essere eliminati.
18. È vietato agli alunni cancellare o alterare file o cartelle presenti sulla postazione utilizzata.
19. Onde evitare perdite di dati, si consiglia comunque di effettuare, appena possibile, copie di sicurezza del lavoro svolto (es. su pendrive personale). Per ragioni di manutenzione potrebbero essere effettuati, secondo necessità e al termine delle attività didattiche, interventi di formattazione (cancellazione dei dati) e reinstallazione del software. Perciò, è opportuno che gli utenti effettuino le copie di sicurezza del proprio lavoro.
20. È vietato scaricare file musicali, foto, filmati e file multimediali, salvo quelli necessari per finalità didattiche e comunque, prima di scaricare documenti o file da Internet è necessario chiedere autorizzazione al docente.
21. Non è possibile utilizzare e/o installare software diverso da quello di cui la scuola è regolarmente dotata di licenza di utilizzo. Non è possibile effettuare copie del software presente nelle postazioni salvo autorizzazione e solo nel caso si tratti di free software. I docenti che hanno necessità di installare programmi sono pregati di contattare il responsabile del laboratorio.
22. Occorre limitare il più possibile l'uso della stampante per evitare spreco di carta e di inchiostro/toner:
    - *non devono essere effettuate continue stampe di prova dei file: appositi comandi ne permettono la visualizzazione a video, quindi stampare solo i documenti finali;*
    - *controllare sempre l' anteprima di stampa;*
    - *stampare solo i documenti importanti;*

- *non stampare pagine web, ma usare copia/incolla e poi stampare il documento dopo relativa formattazione, evitando sprechi di inchiostro e carta;*
- *non utilizzare una stampante diversa da quella configurata e non modificare, comunque, la configurazione della stampante;*
- *non stampare pagine con sfondi uniformi es. diapositive di Power Point;*

utilizzare la modalità risparmio quando è possibile;

- *utilizzare sempre la stampa in B/N, evitando stampe a colori.*

23..Nei laboratori di informatica non devono essere trattati né conservati dati sensibili o giudiziari. Non sono permessi server amministrativi o server Internet in questa rete.
Nell'implementazione delle politiche di sicurezza sul firewall per le reti didattiche è necessario tenere traccia di ogni connessione e dell'accesso degli utenti alla rete.

L'adozione di comportamenti corretti garantisce il buon utilizzo delle attrezzature e ne permette il libero uso.

Piano di miglioramento

L'Istituzione Scolastica si pone come obiettivo principale l'implementazione del sistema di gestione di sicurezza delle informazioni conformemente alla normativa di settore.

24.Guasti, danneggiamenti, ammanchi e disfunzioni in genere dovranno essere subito segnalati alla segreteria che procederà alla necessaria manutenzione e alla contestazione di eventuali addebiti.
25.Proposte di acquisto - Sarà cura del Responsabile di Laboratorio, sentiti gli altri Insegnanti, redigere le proposte di acquisto che, accompagnate da idonea Relazione potranno riguardare:

- acquisti urgenti di modesta entità economica,
- acquisti programmati di materiale di consumo necessario per lo svolgimento delle esercitazioni.
- acquisti da inserire in un Piano di acquisti straordinario (da presentare normalmente entro l'inizio dell'anno scolastico)

26.Al termine dell'anno scolastico il responsabile di laboratorio dovrà comunicare con apposita relazione, le manutenzioni necessarie per rendere ottimale l'utilizzo del Laboratorio per il successivo anno scolastico.
27.Il docente responsabile dei sussidi concorda all'inizio dell'anno scolastico con i collaboratori scolastici incaricati della loro dislocazione nelle classi le modalità di utilizzo:

- registrazione, su specifico registro predisposto, della classe e docente a cui viene consegnato il sussidio e la riconsegna; i collaboratori sono tenuti a passare il modulo al collega che subentra nel turno qualora non sia conclusa l'attività di utilizzo del sussidio (registro uso sussidi)
- spazi di custodia dei sussidi e loro pulizia
- utilizzo esterno alla scuola o in orario extra scolastico

MISURE MINIME PER I TRATTAMENTI CON STRUMENTI ELETTRONICI:

1. ***Autenticazione informatica;***

   L'autenticazione informatica è la prima misura minima da adottare (username e password)
2. ***Adozione di procedure di gestione delle credenziali di autenticazione;***
3. ***Utilizzazione di un sistema di autorizzazione;***
4. ***Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;***
5. ***Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;***
6. ***Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;***
7. ***Adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.***

Altre misure minime da adottare sono elencate nell'allegato B del decreto legislativo:

- **Sistema di Autenticazione Informatica:**

  Il sistema di autenticazione si basa sull'utilizzo di Credenziali (Username e Password) che vengono assegnate o associate individualmente ad ogni incaricato, il quale ha l'obbligo di tutelare la segretezza della password. Al fine di evitare la scelta di password facilmente rintracciabili vengono descritti alcuni vincoli da imporre sulla scelta della password quali:

  1. La password deve essere lunga almeno 8 caratteri
  2. Non deve contenere riferimenti facilmente riconducibili all'incaricato
  3. Deve essere modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni *6* mesi.

  Inoltre le credenziali, in quanto mezzo di identificazione dell'incaricato, permettono l'accesso ad una sessione di trattamento personalizzata dello strumento elettronico associata alle credenziali inserite a cui è assegnata la responsabilità delle azioni svolte in quella sessione, è buona norma quindi non lasciare incustodito e accessibile lo strumento elettronico in caso di assenza anche solo momentanea.
  Infine le credenziali non possono essere assegnate ad altri incaricati neppure in tempi diversi infatti le credenziali non utilizzate da almeno sei mesi devono essere disattivate.

- **Sistema di Autorizzazione**

  Il sistema di autorizzazione permette di individuare profili di autorizzazione di ambito diverso per ciascun incaricato o per classi omogenee di incaricati in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

8. Adozione di procedure di gestione delle credenziali di autenticazione;

9. Utilizzazione di un sistema di autorizzazione;

10. Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

11. Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

12. Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilitàdei dati e dei sistemi;

13. Adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

CODICE PRIVACY – MISURE MINIME

Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
[g) tenuta di un aggiornato documento programmatico sulla sicurezza;]
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari

AUTENTICAZIONE INFORMATICA

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione. Le credenziali di autenticazione possono consistere in:

A) un codice per l'identificazione dell'incaricato associato a una parola chiave riservata;
B) un dispositivo di autenticazione;
C) una caratteristica biometrica dell'incaricato

Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato

CREDENZIALI DI AUTENTICAZIONE

La parola chiave (password) per l'autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
La password non può contenere riferimenti agevolmente riconducibili all'incaricato
La password è modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la password è modificata almeno ogni tre mesi.

Gli incaricati non possono lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. Utilizzare uno screensaver protetto da password.
E' vietato utilizzare lo stesso codice di autenticazione (seppure in tempi diversi) da più di un incaricato.

SOLUZIONI ANTI-INTRUSIONE E ANTI-VIRUS

I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* c.p. (ossia quelli potenzialmente idonei a danneggiare o interrompere il funzionamento dei sistemi informatici o telematici), mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale

AGGIORNAMENTO SOFTWARE

Gli aggiornamenti periodici dei programmi per elaboratore - programmi e sistema operativo - volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti devono essere effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno
semestrale.

BACKUP SETTIMANALE

Almeno una volta alla settimana deve essere eseguito il backup dei dati.
Il backup è un'operazione che permette di conservare i dati (preferibilmente su supporti ottici non riscrivibili) e consente di prevenire inaspettati blocchi del sistema o dannosissime perdite di dati. L'aggiornamento settimanale, tuttavia, potrebbe non bastare. E' sempre consigliabile il backup quotidiano dei dati, anche se fosse soltanto di tipo incrementale su supporti magnetici

Istruzioni operative per l'utilizzo a scopo lavorativo di strumenti informatici assegnati al personale

L'istruzione ha come obiettivo la regolamentazione dell'utilizzo per uso personale degli strumenti informatici, ossia definire in modo puntuale le regole e i confini da non superare nell'uso delle dotazioni.

Tenuto conto delle Linee guida sulla disciplina della navigazione in Internet e sulla gestione della posta elettronica nei luoghi di lavoro emanate dal Garante per la Privacy, con propria deliberazione n. 13 del 1 marzo 2007, il personale dove attenersi alle seguenti istruzioni e raccomandazioni nell'utilizzo del personal computer.

- Il personal computer con i relativi programmi, il telefono, i fax e ogni altro bene della scuola costituiscono strumenti di lavoro il cui utilizzo ricade sotto la responsabilità della scuola stessa, che li mette a disposizione del proprio personale a condizione che vengano custoditi con cura dal dipendente cui sono assegnati, evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone, per scopi non consentiti.

- Non è consentito modificare le configurazioni impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come, ad es., masterizzatori, modem, ecc.).

- Sui personal computer dotati di scheda audio e/o di lettore CD non è consentito l'ascolto di programmi, file audio o musicali, se non a fini prettamente lavorativi.

- Il personal computer deve essere protetto da password di accensione, che deve essere attivata anche per il disco fisso. Lo screensaver deve essere impostato per tempi brevi (15 minuti) e, quando attivato, disinseribile solo tramite password utente.

- Il personal computer deve essere spento prima di lasciare gli uffici e in caso di assenze prolungate o in caso di suo inutilizzo. In ogni caso, 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.

- Non è consentito utilizzare programmi diversi da quelli ufficialmente installati né installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.

- Non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

- Tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte di .....

- Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale addetto nel caso in cui siano rilevati virus e seguendo le procedure di protezione antivirus.

- Tutti i supporti magnetici rimovibili (floppy disk, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni, devono essere trattati con particolare cautela, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

- Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale addetto e seguire le istruzioni da questo impartite.

- In ogni caso, i supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti in armadi chiusi.

- È vietato l'utilizzo di supporti rimovibili personali.

- L'utente è responsabile della custodia dei supporti e dei dati della scuola in essi contenuti.

- Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dall'incaricato delle credenziali, previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

- Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (User Id), assegnato dal personale addetto, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata.

Non è consentita l'attivazione della password di accensione senza preventiva autorizzazione da parte del personale addetto.

- È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi.

- Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con l'incaricato delle credenziali, soggetto preposto alla custodia delle credenziali di autenticazione.

- È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete e ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

- Le unità di rete sono aree di condivisione di informazioni strettamente professionali 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, nemmeno per brevi periodi, in queste unità.

- La scuola si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente Regolamento/ Codice di condotta.

- Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

Istruzioni operative per un giusto comportamento in rete: Netiquette

1. Non usare l'e-mail per alcun proposito illegale o non etico.
2. Non diffondere né spam né messaggi appartenenti a catene di S. Antonio.
3. Includere sempre l'argomento del messaggio in modo chiaro e specifico. Quindi non inviare mai email prive del campo "oggetto"; rispondere sempre alle email, se non altro per dare la conferma al mittente di presa visione.
4. Cercare di rispondere alle email mantenendo sempre lo stesso argomento (topic) per conservare una struttura storica ordinata dei messaggi inviati e ricevuti (thread), "agganciandoli" uno dopo l'altro, evitando possibilmente di spedire un nuovo messaggio per un argomento già in corso di discussione.
5. Seguire le regole di citazione per scrivere la risposta a una email.
6. Firmare sempre col proprio nome alla fine del messaggio, a meno che la Firma non sia già inclusa nell'oggetto.
7. Mantenere la privacy dei mittenti/destinatari, cancellando dal testo l'eventuale indirizzo di posta elettronica del mittente (se si inoltra una email quando il destinatario non dovesse conoscere il mittente originale) e utilizzando la casella Bcc (o Ccn) se si deve inviare a destinatari che non si conoscono tra loro.
8. Non insultare e non fare uso indiscriminato di parole scritte in maiuscolo (esse, infatti, corrispondono al tono di voce alto del parlato, e dunque denotano nervosismo o cattiveria).
9. Riflettere bene su come il destinatario possa reagire al proprio messaggio: valutare se può essere realmente interessato al contenuto e utilizzare eventualmente le emoticon per indicare il tono della conversazione, in particolare se scrivono battute (se è diverso da quello che potrebbe far pensare la semplice lettura del testo).
10. La dimensione del messaggio da inviare non deve essere troppo grande: in genere la sua dimensione dovrebbe rimanere al di sotto di 50-100 kB (al posto di contenuti di grandi dimensioni - immagini, documenti, ... - si possono inserire nel testo del messaggio dei link a tali risorse reperibili in altro modo, per esempio via FTP o HTTP; comunque allegati indicativamente non superiori a 6 MB, in formati diffusi e aperti come .pdf o .jpeg per le immagini, già settati per la stampa, ed eventualmente compressi con programmi nativi del sistema operativo).
11. Non inviare messaggi privati da postazioni dalle quali possono essere letti da altri o, se lo si fa, ricordarsi di eliminare le tracce.

12. Citare il testo a cui si risponde il più brevemente possibile, ma in modo che risulti comunque chiaro in cima alla risposta.
13. Non richiedere indiscriminatamente, per qualsiasi messaggio, la ricevuta di ritorno da parte del destinatario.
14. Non allegare file di dimensioni eccessive e non allegare file con nomi eccessivamente lunghi o che contengono caratteri particolari come quelli di punteggiatura.
15. Non impostare indiscriminatamente, per qualsiasi messaggio, il flag di importante e/o urgente (è come gridare al lupo al lupo inutilmente): con il passare del tempo chi riceverà le tue e-mail ignorerà il flag.
16. Scrivere in modo semplice e diretto, con periodi brevi. Andare a capo spesso perché gli spazi bianchi delle interlinee aiutano la lettura. Fare una lista per punti se ci sono molte cose da dire: il testo così si leggerà facilmente anche su uno smartphone.
17. Salvare il proprio messaggio in bozza quando quest'ultimo viene scritto di getto. Rileggilo il giorno dopo: sicuramente cambierai opinione su quello che hai scritto.
18. Leggere il proprio messaggio almeno tre volte prima di inviarlo e dimostrare di avere almeno letto il messaggio del mittente approfonditamente prima di dare risposte senza pensare.