ISTITUTO COMPRENSIVO MARCO POLO VIANI
Via Pistoia n. 68 Viareggio (LU) - Tel. 0584 51302
c.f. 91022950462 - email luic819009@istruzione.it
www.marcopoloviani.edu.it

REGOLE DI CONDOTTA A TUTELA DELLA PRIVACY E DELLA SICUREZZA DEI DATI PERSONALI

Originale	**Titolare del trattamento**
Revisione n. 0	**Firma**

Sommario

REGOLE DI CONDOTTA A TUTELA DELLA PRIVACY E DELLA SICUREZZA DEI DATI PERSONALI 1

PREMESSA 5

1. PRINCIPI BASE DEL TRATTAMENTO DATI PERSONALI 7

2. GESTIONE DEI DATI PERSONALI 8

REGOLE DI CONDOTTA 9

1. CONTESTO AMBIENTALE 11

2. POSTAZIONE DI LAVORO 11

3. DOCUMENTI E ATTI CARTACEI 11

4. UTILIZZO DEL PERSONAL COMPUTER 13

5. GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE 14

6. UTILIZZO DI SERVER E DEGLI SPAZI DI CONDIVISIONE 15

7. UTILIZZO DI PERSONAL COMPUTER PORTATILI 15

8. USO DELLA POSTA ELETTRONICA 15

9. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI 16

10. PRECAUZIONI CONTRO MALWARE 17

11. UTILIZZO DEI TELEFONI, FAX E FOTOCOPIATRICI DELL'ISTITUTO SCOLASTICO 18

12. CUSTODIA ED USO DI SUPPORTI RIMOVIBILI 18

13. INOSSERVANZA DELLA NORMATIVA DELL'ISTITUTO SCOLASTICO 20

PREMESSA

Il presente disciplinare interno ha l'obiettivo di definire un insieme di norme comportamentali a cui tutti i dipendenti e i collaboratori, che operano per l'istituto, devono uniformarsi nell'ambito delle attività che implicano il trattamento di dati ed informazioni ed evitare, così, condotte inconsapevoli e/o scorrette che potrebbero esporre l'istituto a problematiche di sicurezza, di immagine e patrimoniali, per eventuali danni cagionati anche a terzi.

L'insieme delle norme comportamentali ivi incluse, pertanto, è volto a prevenire comportamenti illeciti dei dipendenti nell'approccio al dato personale, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano.

Il presente disciplinare si applica, quindi, ad ogni Utente assegnatario di beni e risorse informative dell'istituto.

Per ***Utente*** si intende, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore (interno o esterno), consulente, fornitore e/o terzo che in modo continuativo e non occasionale operi all'interno della struttura scolastica utilizzandone beni e servizi informatici.

Per ***Ente*** si intende, invece, la società, l'organizzazione e/o comunque il Titolare dei beni e delle risorse informative, vale a dire, il Titolare del Trattamento, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

1. PRINCIPI BASE DEL TRATTAMENTO DATI PERSONALI

1.1 ***L'attività di trattamento dati personali*** può essere definita come qualunque operazione o complesso di operazioni realizzate su informazioni riferite a persone fisiche. Il trattamento di un dato personale, per essere lecito, corretto e trasparente, deve sempre avvenire secondo alcuni principi generali *privacy*, che possono essere considerati i fari illuminanti di ogni trattamento. È importante chiedersi sempre se questi vincoli siano rispettati e solo ad una risposta positiva possiamo avere la certezza che la *privacy* di un soggetto sia rispettata. In particolare, qualunque trattamento dati personali deve essere effettuato nel rispetto dei principi di:

- ***Tutela della dignità dell'interessato***, cioè della persona fisica di cui le informazioni personali i riferiscono;
- ***Principi di liceità, correttezza e trasparenza***: i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato, in maniera da garantire un'adeguata sicurezza, anche mediante l'adozione di misure tecniche e organizzative adeguate. Quanto alla trasparenza, tutte le informazioni destinate al pubblico o all'interessato devono essere concise, facilmente accessibili e di facile comprensione e il linguaggio utilizzato deve essere semplice e chiaro;
- ***Limitazione della finalità*****:** gli scopi del trattamento devono essere determinati, espliciti e legittimi;
- ***Minimizzazione dei dati***: i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Nello specifico, i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'uso di dati personali, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante dati anonimi o altre opportune modalità che permettano di identificare l'interessato solo in caso di necessità ('principio di necessità');
- ***Esattezza***: i dati trattati devono essere esatti e, se necessario, aggiornati; pertanto, devono

essere adottate tutte le misure ragionevoli per cancellare o rettificare i dati inesatti rispetto alle finalità per le quali sono trattati;

- ***Limitazione della conservazione*****:** i dati trattati devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario al conseguimento degli scopi per cui sono raccolti e trattati;
- ***Integrità e riservatezza***: i dati devono essere trattati in modo da evitare trattamenti illeciti, perdite, distruzioni o alterazioni accidentali mediante l'adozione di idonee misure tecniche-organizzative.

2. GESTIONE DEI DATI PERSONALI

2.1 L'accesso ai dati è consentito nei limiti della propria funzione organizzativa e della propria attività lavorativa.

2.2 Ogni Autorizzato è responsabile dei dati e delle informazioni delle quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi trattare i dati e le informazioni adottando ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza, l'integrità ed il corretto utilizzo. I dati e le informazioni potranno essere comunicate a terze parti esclusivamente nell'ambito della propria funzione e secondo le finalità connesse alla propria attività lavorativa.

2.3 È assolutamente vietata la divulgazione di qualunque informazione appresa nel contesto lavorativo dall'Autorizzato.

2.4 Si ricorda, inoltre, che la diffusione illecita di dati e informazioni potrebbe configurare, oltre alla violazione del presente Regolamento, la violazione di norme con conseguenze sia civili che penali a carico del responsabile dell'illecita diffusione, nonché come violazione della normativa che regola il rapporto di lavoro.

REGOLE DI CONDOTTA

1. CONTESTO AMBIENTALE

1.1 Tutti i locali e tutti gli asset dell'istituto devono essere utilizzati e custoditi con la massima diligenza al fine di garantire un'efficiente conduzione dell'attività lavorativa ed un adeguato livello di sicurezza delle informazioni, attenendosi al presente Regolamento per garantire la sicurezza fisica delle aree e degli archivi del Titolare del trattamento.

1.2 L'accesso agli uffici, alle aree protette, alle aree riservate ed agli archivi fisici, è permesso ai soli soggetti a ciò autorizzati in forza delle mansioni cui sono adibiti. Ulteriori e specifici accessi ad uffici ed aree protette potranno essere concessi e abilitati da parte del Titolare del trattamento solo a seguito di preventiva e motivata richiesta. I visitatori e gli ospiti di vario genere potranno avere accesso alle suddette aree solo accompagnati da un Autorizzato che, in ogni caso, sarà tenuto a vigilare sulla condotta del terzo.

2. POSTAZIONE DI LAVORO

2.1 Per postazione di lavoro si intende il complesso unitario di Personal Computer, notebook, accessori, periferiche e ogni altro devices concesso, dall'istituto, in utilizzo all'Utente.

2.2 Il PC e gli altri dispositivi di cui sopra devono essere utilizzati con hardware e software autorizzati dall'istituto.

2.3 L'utilizzo della postazione di lavoro e il conseguente accesso ai documenti, atti, archivi, banche dati è consentito nei limiti della propria funzione, dei propri incarichi e delle proprie mansioni.

2.4 Le postazioni di lavoro non devono essere lasciate incustodite con le sessioni utenti attive; quando un Utente si allontana dalla propria postazione di lavoro, deve bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password o effettuare il log-out dalla sessione.

2.5 I documenti cartacei non devono essere lasciati incustoditi sulla scrivania e/o in luoghi aperti al pubblico in assenza di altri autorizzati addetti al medesimo trattamento.

2.6 E' fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici dell'istituto a soggetti terzi.

2.7 Gli apparecchi di proprietà personale dell'Utente quali computer portatili, telefoni cellulari, agende palmari (PDA), hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali, ecc. non potranno essere collegati ai computer o alle reti informatiche della scuola, salvo preventiva autorizzazione del Titolare del trattamento.

3. DOCUMENTI E ATTI CARTACEI

3.1 L'istituto ha messo a disposizione appositi locali ed archivi ad accesso selezionato (di seguito "luogo sicuro"), ove devono essere custoditi i documenti contenenti dati personali;

3.2 I documenti e gli atti contenenti dati appartenenti a particolari categorie e giudiziari devono essere custoditi in armadi chiusi a chiave.

3.3 In generale, i documenti non devono essere asportati da tale luogo sicuro e, ove ciò avvenga, l'asportazione deve essere ridotta al minimo tempo necessario per effettuare le operazioni di trattamento e in accordo con le seguenti cautele operative:

- Dal luogo sicuro devono essere asportati solo i documenti strettamente necessari per le operazioni di trattamento e non intere pratiche, se ciò non è necessario.
- Al termine delle operazioni di trattamento, i documenti devono essere immediatamente riposti nel luogo sicuro.
- Per tutto il periodo in cui i documenti sono all'esterno del luogo sicuro, l'Autorizzato non deve mai perderli di vista, adempiendo ad un preciso obbligo di custodia dei documenti stessi.
- L'Autorizzato deve, inoltre, controllare che i documenti composti da numerose pagine o più raccoglitori siano sempre completi, verificando sia il numero dei fogli che l'integrità del contenuto rispetto a quanto presente all'atto del prelievo dal luogo sicuro.
- I documenti di cui sopra non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.
- Adottare le cautele necessarie per evitare che terzi estranei possano venire a conoscenza del contenuti dei documenti.
- I documenti non possono esser riprodotti o fotocopiati se non per esigenze connesse alla finalità del trattamento.
- Limitare al minimo assoluto il numero di fotocopie effettuate.
- Adottare una procedura per la consegna delle copie ai destinatari che dia tutte le garanzie di sicurezza; in particolare, dovranno essere adoperate buste di sicurezza sigillate, oppure la consegna dovrà essere effettuata personalmente, in modo da ridurre al minimo la possibilità che soggetti terzi non autorizzati possano prendere visione del contenuto.
- Particolare cautela deve essere posta ove i documenti in questione vengano consegnati in originale.
- I documenti contenenti dati appartenenti a particolari categorie o dati che, per una qualunque ragione, siano stati indicati dal Titolare o dal Responsabile come meritevoli di particolare attenzione devono, in fase di affidamento, essere custoditi con la maggior diligenza possibile.
- In caso di consegna postale dei documenti, accertarsi che il destinatario abbia effettivamente ricevuto la missiva e che il suo contenuto risulti integro.
- Eventuali fotocopie o documenti non riusciti debbono essere distrutti in modo tale da non consentire la ricostruzione del contenuto.
- E' tassativamente proibito utilizzare le fotocopie non riuscite come carta per appunti.
- E' parimenti tassativamente proibito trasportare all'esterno del posto di lavoro fotocopie non riuscite, da utilizzare altrove come carta per appunti.

- Gli atti o i documenti contenenti dati personali non devono essere trasportati fuori dal luogo di lavoro in mancanza di autorizzazione o permesso rilasciato dal Titolare del trattamento o dal Responsabile.
- Nel caso in cui sia autorizzato il trasporto della documentazione fuori dal luogo di lavoro, è necessario che l'Autorizzato salvaguardi la riservatezza dei dati personali adoperando le seguenti cautele:

  - i documenti devono essere riposti in buste chiuse o in una borsa;

  - la busta o la borsa nella quale sono contenuti i documenti da trasportare deve essere sempre tenuta con sé dall'Autorizzato, non deve essere mai lasciata incustodita.
- E' tassativamente proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il corrispondente sia un soggetto a ciò Autorizzato.

3.4 Qualora sia necessario distruggere i documenti contenenti dati personali, devono essere utilizzati gli appositi apparecchi "distruggi documenti"; in assenza di tali strumenti, i documenti devono essere sminuzzati in modo da non essere più ricomponibili.

3.5 I documenti non devono essere lasciati incustoditi presso i dispositivi di stampa

3.6 In caso di dubbio sulle modalità di applicazione di quanto sopra illustrato, o per chiedere ulteriori chiarimenti in merito, l'Autorizzato deve rivolgersi al Titolare del trattamento.

4. UTILIZZO DEL PERSONAL COMPUTER

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

4.2 L'accesso all'elaboratore è protetto da password che deve essere custodita dall'utente con la massima diligenza e non divulgata.

4.3 Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione del Titolare del trattamento (o persona/ufficio dallo stesso incaricata), in quanto sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

4.4 Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Titolare del trattamento (o persone/ufficio dallo stesso incaricata). L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'istituto a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (Legge 633/1941 e successive modifiche, D.Lgs. 518/1992 sulla tutela giuridica del software, Legge 248/2000 nuove norme di tutela del diritto d'autore, Legge 128/2004 e successive modifiche) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

4.5 Non è consentito all'utente modificare le caratteristiche impostate sul proprio Personal Computer, salvo previa autorizzazione esplicita del Titolare del trattamento (o persona/ufficio dallo stesso incaricata).

4.6 E' onere dell'Utente, in relazione alle sue competenze, eseguire richieste di aggiornamento sulla

propria postazione di lavoro derivanti da software antivirus nonché sospendere ogni attività in caso di minacce virus o altri malfunzionamenti, segnalando prontamente l'accaduto all'amministratore del sistema o al Titolare del trattamento.

4.7 Gli strumenti dovranno essere automaticamente spenti o messi in modalità a basso consumo se non usati per più di mezz'ora e la loro riattivazione sarà consentita sola a seguito di re-immissione delle credenziali di accesso personali.

4.8 Il Personal Computer deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. 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'uso indebito. In ogni caso deve essere attivato lo screen saver e la relativa password.

4.9 Qualsiasi strumento informatico deve essere custodito dall'Autorizzato con cura e diligenza, prevenendo possibili danneggiamenti che ne compromettano il corretto funzionamento ed evitando di lasciarli incustoditi in ambienti pubblici. In caso di furto o danneggiamento di beni, l'Autorizzato dovrà informare immediatamente il Titolare del trattamento.

5. GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

5.1 Le credenziali di autenticazione per l'accesso alla rete e per altri servizi vengono assegnate dal Titolare del trattamento (o persona/ufficio dallo stesso incaricata). Esse consistono in un codice per l'identificazione dell'Utente (username), associato ad una parola chiave (password) riservata che dovrà essere custodita dall'Autorizzato con la massima diligenza e non divulgata. Ogni Autorizzato è responsabile della sicurezza e di qualunque operazione effettuata utilizzando le proprie credenziali. Non possono essere utilizzate le credenziali appartenenti ad altri utenti, nemmeno se sono state comunicate da questi ultimi.

5.2 E' necessario procedere alla modifica della password a cura dell'Autorizzato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati appartenenti a particolari categorie e dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi.

5.3 Le password devono rispettare le seguenti regole:

- Lunghezza di almeno 15 caratteri (o se consentita una lunghezza inferiore utilizzare la lunghezza massima prevista), ricordando che maggiore è la lunghezza, maggiore è la sicurezza della password;
- Presenza di lettere minuscole (a-z);
- Presenza di lettere maiuscole (A-Z);
- Presenza di numeri arabi (0-9);
- Presenza caratteri speciali (ad esempio !, ?, #, *);
- Evitare di includere parti del nome, cognome o comunque elementi agevolmente riconducibili all'utente;
- Evitare l'utilizzo di password comuni o prevedibili;

5.4 È vietato annotare le password su post it o altri supporti.

5.5 Se l'Utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, lo stesso è tenuto a modificare immediatamente la password e/o a segnalare la violazione al Titolare del trattamento (o persona/ufficio dallo stesso incaricata).

5.6 Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Titolare del trattamento (o persona/ufficio dallo stesso incaricata).

5.7 In caso di interruzione del rapporto di lavoro con l'Utente, le credenziali di autenticazione di cui sopra verranno disabilitate immediatamente; entro sei mesi, invece, si disporrà la definitiva e totale cancellazione dell'account Utente.

6. UTILIZZO DI SERVER E DEGLI SPAZI DI CONDIVISIONE

6.1 Le unità di rete o le cartelle condivise sono aree contenenti 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. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup.

6.2 Le password d'ingresso alla rete ed ai programmi sono personali e vanno gestite secondo le procedure impartite. E' assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

6.3 La memorizzazione temporanea di dati su strumenti informatici privati è consentita a patto che i suddetti strumenti siano protetti in modo da non consentire l'accesso di estranei non autorizzati.

6.4 Il Titolare del trattamento (o persona/ufficio dallo stesso incaricata) può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza dei Personal Computer.

6.5 Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

7. UTILIZZO DI PERSONAL COMPUTER PORTATILI

7.1 L'utente è responsabile del Personal Computer portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

7.2 Ai Personal Computer portatili si applicano le regole di utilizzo previste per i Personal Computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

7.3 I Personal Computer utilizzati all'esterno (convegni, visite in istituto, ecc.) in caso di allontanamento, devono essere custoditi in luogo protetto.

8. USO DELLA POSTA ELETTRONICA

8.1 La casella di posta, assegnata dall'istituto, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 E' fatto divieto di utilizzare le caselle di posta elettronica dell'istituto per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

8.3 E' buona norma evitare messaggi estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili o soprattutto allegati ingombranti.

8.4 Il contenuto dei messaggi di posta inviati e ricevuti con mail dell'istituto (anche del tipo

nome.cognome@nomeistituto.it) non deve essere considerato confidenziale e riservato.

8.5 Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica dell'istituto e sono tenuti ad utilizzarla in modo conforme alle presenti regole. Gli stessi, pertanto, devono:

a) conservare la password nella massima riservatezza e con la massima diligenza;

b) mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;

c) prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché alla posta ricevuta.

d) prestare attenzione agli allegati provenienti da mittenti sconosciuti, in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (ad esempio virus, trojan ecc);

e) inviare preferibilmente files in formato PDF;

f) accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i files attachment di posta elettronica prima del loro utilizzo;

g) collegarsi a siti internet contenuti all'interno di messaggi solo quando vi sia comprovata sicurezza sul contenuto degli stessi.

8.6 Nel caso in cui l'e-mail debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:

a) l'indirizzo del destinatario sia stato correttamente digitato;

b) l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;

c) nel caso in cui il documento contenente dati particolari sia un allegato alla e-mail, questo deve essere protetto da password, precedentemente concordata con il destinatario e comunicata attraverso un diverso canale.

8.7 Il Titolare del trattamento prevede che ad ogni messaggio in uscita sia automaticamente aggiunto un breve testo di avviso al ricevente della natura riservata del messaggio.

8.8 E' vietato inviare catene telematiche (o di Sant'Antonio). Non si devono in alcun caso attivare gli allegati di tali messaggi.

8.9 Il Titolare del trattamento, o persona da lui incaricata, potrà occasionalmente visionare il contenuto delle mail dell'istituto se questo si renda strettamente necessario per fini di sicurezza informatica o per improrogabili esigenze lavorative.

8.10 Nel caso di cessazione del rapporto di lavoro con l'utente la casella di posta elettronica assegnata all'autorizzato sarà disattivata con contestuale adozione di un messaggio automatico volto ad informare i terzi del mancato recapito e ad indicare un account alternativo per contattare il Titolare del trattamento.

9. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

9.1 Ogni Utente potrà essere abilitato, dall'istituto, alla navigazione Internet tramite la rete della scuola. Col presente disciplinare, si richiama gli utenti ad una particolare attenzione nell'utilizzo di Internet e dei servizi relativi, in quanto ogni operazione posta in essere è associata all'Indirizzo Internet Pubblico

assegnato all'istituto.

9.2 Internet è uno strumento messo a disposizione degli utenti per uso professionale. Ciascun lavoratore, pertanto, deve usare la rete Internet in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; l'Utente deve quindi prendere ogni precauzione a tale riguardo.

9.3 Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

a) L'utilizzo è consentito esclusivamente per scopi lavorativi e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative.

b) Non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi espressamente autorizzati dall'istituto.

c) È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

d) Non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in guest-book, anche utilizzando pseudonimi (o nicknames).

e) Non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

f) E' consentito l'utilizzo di soluzioni di Instant Messanger e/o chat esclusivamente per scopi professionali ed attraverso gli strumenti ed i software messi a disposizione dall'istituto.

g) Non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo.

h) Non è consentito lo scambio e/o la condivisione (es. i c.d. sistemi di Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da copyright.

i) Non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'istituto in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente.

l) È proibito rigorosamente qualsiasi uso del Web e dei social network che non trasmetta un'immagine positiva o che possa in qualunque modo risultare nocivo all'immagine dell'istituto.

9.4 Per facilitare il rispetto delle predette regole, l'istituto si riserva la facoltà di configurare specifici filtri che inibiscono l'accesso a siti o contenuti ivi non consentiti (con esclusione dei siti istituzionali) e che prevengono operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di file o software).

10. PRECAUZIONI CONTRO MALWARE

10.1 Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'istituto mediante virus o altro software malefico. In particolare l'utente deve:

- limitare allo stretto necessario lo scambio fra computer di file con estensione: exe, dll, zip, com, bat, chm, cpl, hlp, hta, ink, ocx, pif, reg, scr, url, vbs, rar;

- non aprire gli allegati di posta se non si è certi della loro provenienza;
- non cliccare mai un link presente in un messaggio di posta elettronica di provenienza sconosciuta;
- non cliccare mai, durante la navigazione Internet, su banner o link pubblicitari non necessari per l'attività lavorativa;
- provvedere all'installazione degli aggiornamenti richiesti dai software presenti sull'elaboratore, qualora la loro messa in opera sia rilasciata all'iniziativa dell'utilizzatore.

10.2 Ogni anomalia o problematica relativa a malware dovrà essere prontamente segnalata al Titolare del trattamento (o persona/ufficio dallo stesso incaricata). Nel caso il software antivirus rilevi la presenza di un file infetto non bonificato, l'utente dovrà immediatamente sospendere ogni elaborazione in corso – senza spegnere il Personal Computer - e segnalare l'accaduto.

11. UTILIZZO DEI TELEFONI, FAX E FOTOCOPIATRICI DELL'ISTITUTO SCOLASTICO

11.1 Il telefono dell'istituto affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa.

11.2 Qualora venisse assegnato un cellulare dell'istituto all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare dell'istituto si applicano le medesime regole sopra previste per l'utilizzo del telefono dell'istituto: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.

11.3 L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare dell'istituto è possibile soltanto in presenza di preventiva autorizzazione scritta del Titolare del trattamento.

11.4 E' vietato l'utilizzo dei fax dell'istituto per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Titolare del trattamento.

11.5 E' vietato l'utilizzo delle fotocopiatrici dell'istituto per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Titolare del trattamento.

11.6 E' cura dell'Autorizzato effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. E' buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

11.7 E' richiesta una particolare attenzione quando si invia su una stampante condivisa documenti aventi ad oggetto dati personali o informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampa.

12. CUSTODIA ED USO DI SUPPORTI RIMOVIBILI

12.1 In linea generale, non è consentita la copia su supporti rimuovibili di dati appartenenti a particolari categorie e dati giudiziari, per ridurre al minimo il rischio di perdita o distruzione anche accidentale dei dati stessi.

Infatti, non si deve dimenticare che un supporto rimovibile smarrito e/o accidentalmente incustodito, anche per breve periodo, può essere rapidamente letto e copiato, senza lasciare alcuna traccia

dell'accaduto, trovandosi davanti un rischio concreto di accesso non autorizzato o copia abusiva dei dati sensibili e giudiziari.

Ciò premesso, ove nello svolgimento dell'attività assegnata all'Autorizzato sia indispensabile effettuare una copia di dati, e ciò sia stato specificamente consentito dal Titolare del trattamento, occorre attenersi alle seguenti cautele:

- Accertarsi che il supporto rimovibile sia debitamente formattato e privo di altri file, che potrebbero essere infetti. Nel dubbio, è buona norma provvedere alla formattazione ex novo prima di registrare dati personali.
- Il supporto rimovibile, se possibile, deve essere contrassegnato da un'etichetta con l'indicazione in codice del suo contenuto.
- Il supporto rimovibile contente dati appartenenti a particolari categorie e giudiziari deve essere sempre direttamente e personalmente custodito dall'incaricato che ha realizzato la copia.
- In caso di spedizione al altro incaricato, occorre accertarsi che il destinatario abbia lo stesso profilo di autorizzazione del mittente e che il supporto rimovibile venga spedito in una busta sigillata, intestata personalmente all'incaricato, con controfirma sul lembo di chiusura.
- Non si deve spedire un supporto rimovibile contenente dati particolari ad un destinatario, senza aver prima concordato con il destinatario stesso le modalità e tempi di consegna ed aver stabilito la procedura che permette di confermare l'avvenuta consegna al destinatario del supporto stesso.
- Qualora i dati contenuti sul supporto rimovibile non abbiamo più ragione di essere, si deve provvedere immediatamente alla formattazione del supporto rimovibile ed alla asportazione dell'etichetta con la indicazione del contenuto od alla sua cancellazione.
- Poiché i supporti rimovibili sono particolarmente sensibili ai campi magnetici, per evitare la cancellazione o danneggiamento, anche accidentali, dei dati, il supporto rimovibile non deve mai essere avvicinato ad un campo magnetico, oppure lasciato abbandonato nelle vicinanze di un trasformatore.
- I supporti rimovibili contenenti dati personali non devono essere esposti ad estremi di temperatura e di umidità.
- Prestare attenzione a non dimenticare il supporto rimovibile all'interno del computer quando, al termine della copia, si spegne il computer e ci si allontana.
- Se l'operazione è ragionevolmente possibile, si raccomanda vivamente di compilare un registro con l'indicazione numerica, o con altro contrassegno, ove sono riportati tutti i supporti rimovibili contenenti dati sensibili e giudiziari, la loro ubicazione, le modalità di accesso, gli eventuali estremi di consegna ad altro incaricato autorizzato.
- Il supporto rimovibile contenente dati appartenenti a particolari categorie o giudiziari non deve mai essere lasciato abbandonato sul tavolo, ma deve essere immediatamente posto all'interno di una custodia sicura. Quando non utilizzato, in funzione della criticità dei dati archiviati, si può riporre da un cassetto della scrivania chiuso a chiave, sino ad un armadio blindato od una cassaforte, idonea alla custodia di supporti magnetici.
- Conservare il supporto di memoria esterno in luogo diverso rispetto a quello in cui si trovano gli

elaboratori in cui sono trattati i dati.

13. INOSSERVANZA DELLA NORMATIVA DELL'ISTITUTO SCOLASTICO

13.1 Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari, in base a quanto previsto dall'art. 7 dello Statuto dei Lavoratori, nonché con le azioni civili e penali previste dalla Legge.