ISTITUTO COMPRENSIVO STATALE DI LOZZO ATESTINO
Scuole dell'Infanzia, Primarie e Secondarie di I grado di Lozzo Atestino, Cinto Euganeo e Vo'
Via G. Negri, 3 – 35034 LOZZO ATESTINO (PD) C.F. 82005950280
Segreteria Tel. 0429 94097 Fax 0429 647839 e-mail pdic85700d@istruzione.it
Codice Ministeriale PDIC85700D – Sito Web http://www.iclozzoatestino.edu.it/

ISTITUTO COMPRENSIVO STATALE
DI LOZZO ATESTINO
Prot. 0005098 del 23/09/2019
A-A23 (Uscita)

Comunicazione interna n. 43

All'Albo
Al Sito Web

DISCIPLINARE RELATIVO ALL'UTILIZZO DEI DATI

Regole di condotta ed obblighi dei responsabili ed incaricati del trattamento dei dati personali, in relazione all'uso degli strumenti informatici, di Internet e della Posta Elettronica, redatto ai sensi del provvedimento del Garante della Privacy (Deliberazione n. 13 del 1/3/2007 - pubblicata in GU n. 58 del 10 marzo 2007) comprensivo di alcune note per la gestione dei dati cartacei ed adeguato al Regolamento Europeo 679/2016.

1. SEZIONE I AMBITO GENERALE

1.1. Definizioni Ente/organizzazione/Istituto: ISTITUTO COMPRENSIVO DI LOZZO ATESTINO

Autorizzazione : il provvedimento adottato dal Garante con cui il titolare del trattamento (ente pubblico, impresa, libero professionista) viene autorizzato a trattare determinati dati "sensibili" o giudiziari, ovvero a trasferire dati personali all'estero. **Comunicazione:** far conoscere dati personali a uno o più soggetti determinati (che non siano l'interessato, il responsabile o l'incaricato), in qualunque forma, anche attraverso la loro messa a disposizione o consultazione (vedi anche diffusione) **Consenso:** la libera manifestazione di volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, del quale è stato preventivamente informato da chi ha un potere decisionale sul trattamento (vedi titolare).

D.Lgs. 196/2003: Decreto Legislativo 196 del 30 giugno 2003 e sue successive modifiche ed integrazioni.

Dato personale: qualsiasi informazione che riguardi persone fisiche identificate o che possono essere identificate anche attraverso altre informazioni, ad esempio, attraverso un numero o un codice identificativo. Sono, ad esempio, dati personali: il nome e cognome o denominazione; l'indirizzo, il codice fiscale; ma anche un'immagine, la registrazione della voce di una persona, la sua impronta digitale, i dati sanitari, i dati bancari, ecc.

Dato sensibile: un dato personale che, per la sua natura, richiede particolari cautele: sono dati sensibili quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'adesione a partiti, sindacati o associazioni, lo stato di salute e la vita sessuale delle persone.

Dato giudiziario: i dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, ad es., i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione). Rientrano in questa categoria anche la qualità di imputato o di indagato.

Diffusione: divulgare dati personali al pubblico o, comunque, ad un numero indeterminato di soggetti (ad esempio, è diffusione la pubblicazione di dati personali su un quotidiano o su una pagina web).
Dipendente: personale dell'Istituto assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.
GDPR General Data Protection Regulation - Regolamento Generale sulla Protezione dei Dati – UE 2016/679: è un Regolamento con il quale la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione Europea e dei residenti nell'Unione Europea, sia all'interno che all'esterno dei confini dell'Unione europea (UE). Il testo, pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, ha efficacia a partire dal 25 maggio 2018.
Incaricato: ogni dipendente, come sopra identificato, ed ogni consulente esterno che, nell'ambito dell'attività assegnatagli, tratta dati (nell'accezione del capitolo seguente) riferiti all'Istituto. Il regolamento europeo non prevede espressamente la figura dell'incaricato, ma non ne esclude la nomina, facendo riferimento a persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile (art. 4). In sede europea, alla nostra DPA è stato concesso di poter utilizzare ancora i termini titolare, responsabile e incaricato; traducendo così, nella versione italiana del GDPR, la figura del "controller" (Art. 4.7) con "titolare del trattamento"; "processor" (Art. 4.8) con "responsabile del trattamento"; "third party" (Art. 4.10) con "terzo", e di poter continuare ad utilizzare il termine "incaricato" per qualificare "le persone autorizzate al trattamento dei dati 3 personali sotto l'autorità diretta del titolare o del responsabile". Alla luce di ciò, si può identificare la figura di Incaricato in quella di Responsabile.
Informativa: le informazioni che il titolare del trattamento deve fornire ad ogni interessato, verbalmente o per iscritto quando i dati sono raccolti presso l'interessato stesso, oppure presso terzi. L'informativa deve precisare sinteticamente e in modo colloquiale quali sono gli scopi e le modalità del trattamento; se l'interessato è obbligato o no a fornire i dati; quali sono le conseguenze se i dati non vengono forniti; a chi possono essere comunicati o diffusi i dati; quali sono i diritti riconosciuti all'interessato; chi sono il titolare e l'eventuale responsabile del trattamento e dove sono raggiungibili (indirizzo, telefono, fax, ecc.).
Interessato: la persona fisica cui si riferiscono i dati personali.
Misure di sicurezza: sono tutti gli accorgimenti tecnici ed organizzativi, i dispositivi elettronici o i programmi informatici utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti.
NDA: non-disclosure agreement, ovvero accordo di non divulgazione, è un negozio giuridico di natura sinallagmatica che designa informazioni confidenziali e con il quale le parti si impegnano a mantenerle segrete, pena la violazione dell'accordo stesso e il decorso di specifiche clausole penali in esso contenute.

Responsabile (del trattamento): la persona, la società, l'ente, l'associazione o l'organismo cui il titolare affida, anche all'esterno, per la particolare esperienza o capacità, compiti di gestione e controllo del trattamento dei dati.
Titolare del trattamento: la persona fisica, l'impresa, l'ente, l'associazione, ecc. cui fa capo effettivamente il trattamento di dati personali e spetta assumere le decisioni fondamentali sugli scopi e sulle modalità del trattamento medesimo (comprese le misure di sicurezza). Nei casi in cui il trattamento sia svolto da una società o da una pubblica amministrazione per titolare va intesa l'entità nel suo complesso e non l'individuo o l'organo che l'amministra o la rappresenta (presidente, amministratore delegato, sindaco, ministro, direttore generale, ecc.).
Trattamento (di dati personali): un'operazione o un complesso di operazioni che hanno per oggetto dati personali.

1.2. Premessa L'ambito lavorativo porta la nostra organizzazione a gestire una serie di "informazioni", proprie e di terzi, per poter erogare i servizi che le vengono istituzionalmente richiesti. 4 Tali informazioni possono essere considerate, ai sensi del D. Lgs. 196/2003 e s.m.i., "dati personali" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che l'Istituto adotti una serie di misure minime ed idonee previste dalle norme. Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "informazioni riservate", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'organizzazione è chiamata a garantire la riservatezza, o per NDA, o per una più ampia tutela del patrimonio dell'Istituto. Ai fini di questo disciplinare si specifica, pertanto, che con il termine "dati" deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge. Inoltre, nell'ambito della sua attività, l'Istituto tratta "dati cartacei", ovvero informazioni su supporto cartaceo, e "dati digitali", ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali. In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'incaricato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'organizzazione stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita dell'Istituto. Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta. La progressiva diffusione delle nuove tecnologie informatiche ed, in particolare, l'accesso alla rete internet dal computer aziendale, espone l'Istituto a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'organizzazione stessa. Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza,

l'Istituto ha adottato il presente Disciplinare Interno, diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali. Il presente Disciplinare Interno si applica ai Responsabili e Incaricati che si trovino ad operare con dati dell'Istituto. Una gestione dei dati cartacei, un uso dei COMPUTER e di altre attrezzature elettroniche (di seguito DISPOSITIVI), nonché dei servizi internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare potrebbe esporre l'organizzazione ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico. Le informazioni contenute nel presente Disciplinare vengono rilasciate ai sensi dell'art. 13 del Codice sulla Privacy e dell'art. 13 del Regolamento Europeo 679/2016, e costituiscono, quindi, parte integrante dell'informativa rilasciata ai Responsabili ed agli Incaricati.

1.3. Esclusione all'uso degli strumenti informatici All'inizio del rapporto lavorativo o di consulenza, l'Istituto valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari dispositivi aziendali, di internet e della posta elettronica da parte degli incaricati. Successivamente, e periodicamente, l'Istituto valuta la permanenza dei presupposti per l'utilizzo dei dispositivi aziendali, di internet e della posta elettronica. È fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici aziendali. I casi di esclusione possono riguardare: 1. L'utilizzo del COMPUTER o di altri DISPOSITIVI. 2. L'utilizzo della posta elettronica. 3. L'accesso a internet. 5 Le eventuali esclusioni sono strettamente connesse al principio della natura aziendale e lavorativa degli strumenti informatici, nonché al principio di necessità di cui al Codice Privacy e GDPR. Più specificatamente, hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo i responsabili che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno. I casi in cui le esclusioni dovranno risultare operative in forza di tali motivazioni verranno comunicati individualmente e potranno riguardare sia tutti i casi sopra descritti, sia solo uno o due degli stessi Si informa che tali esclusioni sono divenute necessarie alla luce del Provvedimento del Garante 1° marzo 2007, che indica di ridurre a titolo cautelativo e preventivo l'utilizzo degli strumenti informatici in considerazione dei pericoli e delle minacce indicate in questo documento.

1.4. Titolarità dei dispositivi e dei dati L'organizzazione è esclusiva titolare e proprietaria dei dispositivi messi a disposizione dei responsabili, ai soli fini dell'attività lavorativa. L'Istituto è l'unico esclusivo titolare e proprietario di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri dispositivi digitali o archiviati in modo cartaceo nei propri locali. Il Responsabile non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei dispositivi aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo

possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'organizzazione.

1.5. Finalità nell'utilizzo dei dispositivi I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità del Responsabile esclusivamente per un fine di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle istituzionali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare. Qualsiasi eventuale tolleranza da parte di questo Istituto, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

1.6. Restituzione dei dispositivi A seguito di una cessazione del rapporto lavorativo o di consulenza del Responsabile con l'organizzazione o, comunque, al venir meno, ad insindacabile giudizio dell'Istituto, della permanenza dei presupposti per l'utilizzo dei dispositivi aziendali, i responsabili hanno i seguenti obblighi: 1. Procedere immediatamente alla restituzione dei dispositivi in uso. 2. Divieto assoluto di formattare o alterare o manomettere o distruggere i dispositivi assegnati o rendere inintelligibili i dati in essi contenuti, tramite qualsiasi processo.

1.7. Restituzione dei dati cartacei A seguito di una cessazione del rapporto lavorativo o di consulenza del responsabile con l'organizzazione o, comunque, al venir meno, ad insindacabile giudizio dell'Istituto, della permanenza dei presupposti per l'utilizzo di dati cartacei aziendali, gli incaricati hanno i seguenti obblighi: 1. Procedere immediatamente alla restituzione dei dati cartacei in loro possesso. 2. Divieto assoluto di alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili, tramite qualsiasi processo. 6 2.

SEZIONE II PASSWORD

2.1. Le Password Le password possono essere un metodo di autenticazione assegnato dall'organizzazione per garantire l'accesso protetto ad uno strumento hardware, oppure ad un applicativo software. La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e dell'Istituto nel suo complesso. Nel tempo, anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza, generalmente ogni 3 mesi. L'Istituto ha implementato alcuni meccanismi che permettono di aiutare e supportare gli Incaricati in una corretta gestione delle password, in particolare, per quanto riguarda le password di accesso ad ogni dispositivo utilizzato (sia fisico che on line), in particolare nel settore amministrativo. Password che vengono aggiornate periodicamente secondo il livello di sicurezza richiesto dall'Istituto stesso e, comunque, in linea con quanto richiesto dalla normativa privacy. Altra buona norma è quella di non memorizzare la

password su supporti facilmente intercettabili da altre persone. Il miglior luogo in cui conservare una password è la propria memoria. Le password che non vengono utilizzate da parte dei responsabili per un periodo superiore ai sei mesi, verranno disattivate dall'Istituto. In qualsiasi momento, l'organizzazione si riserva il diritto di revocare al responsabile il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

2.2. Regole per la corretta gestione delle password Il responsabile, da parte sua, per una corretta e sicura gestione delle proprie password, deve rispettare le regole seguenti: 1. Le password sono assolutamente personali e non vanno mai comunicate ad altri. 2. Occorre cambiare immediatamente una password, non appena si abbia alcun dubbio che sia diventata poco "sicura". 3. Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali e numeri. 4. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare). 5. Le password devono essere sostituite almeno nei tempi indicati dalla normativa, di norma ogni 3 mesi, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password. 6. Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'Istituto. In particolare, evitare di digitare la password con la LIM accesa, in classe, sul PC collegato alla LIM. In alcuni casi, sono implementati meccanismi che consentono al responsabile un numero limitato di tentativi errati di inserimento della password, oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per alcuni minuti. In caso di necessità, contattare il Titolare.

3. SEZIONE III OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

In questa sezione vengono trattate le operazioni a carico del Responsabile e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto 7 della sicurezza e dell'integrità del patrimonio aziendale.

3.1. Login e Logout Il "Login" è l'operazione con la quale il Responsabile si connette al sistema informativo aziendale o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es.applicativi web, Intranet), ognuno dei quali richiede uno username e una password. In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico user name e password, l'Istituto potrà assegnare un univoco user name e password per gruppi di responsabili per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati. Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o

l'accesso agli stessi da parte di persone non autorizzate. Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla.

3.2. Obblighi L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale. Il responsabile deve quindi eseguire le operazioni seguenti: 1. Se si allontana dalla propria postazione, dovrà mettere in protezione il suo dispositivo affinché persone non autorizzate non abbiano accesso ai dati protetti. 2. Bloccare il suo dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione; 3. Chiudere la sessione (Logout) a fine giornata; 4. Spegnere il PC dopo il Logout; 5. Controllare sempre che non vi siano persone non autorizzate nelle vicinanze che possano prendere visione delle schermate del suo dispositivo.

4. SEZIONE IV USO DEL PERSONAL COMPUTER DELL'ENTE

4.1. Modalità d'uso del COMPUTER aziendale Il sistema informativo aziendale è composto da un insieme di unità (server centrali e client) connessi ad una rete locale (LAN e/o WAN), che utilizzano diversi sistemi operativi e applicativi. I file creati, elaborati o modificati sul computer assegnato devono essere poi sempre salvati a fine giornata sul sistema di repository documentale centralizzato. L'Istituto non effettua il backup dei dati memorizzati in locale.

4.2. Corretto utilizzo del COMPUTER aziendale Il computer consegnato al responsabile è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza. L'accesso all'elaboratore è protetto da password che deve essere custodita dall'responsabile con la massima diligenza e non divulgata. Per necessità aziendali, gli amministratori di sistema utilizzando la propria login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alle memorie di massa locali di rete (repository e 8 backup) che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche in remoto. In particolare il Responsabile deve adottare le seguenti misure: 1. Utilizzare solo ed esclusivamente le aree di memoria della rete dell'Istituto ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri file fuori dalle unità di rete. 2. Spegnere il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché 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. 3. Non dare accesso al proprio computer ad altri utenti, a meno che siano responsabili con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

4.3. Divieti Espressi sull'utilizzo del COMPUTER Al responsabile è vietato: 1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali del responsabile o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere. 2. Modificare le configurazioni già impostate sul personal computer. 3. Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dell'Istituto. 4. Installare alcun software di cui l'Istituto non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione dell'organizzazione. È, peraltro, vietato fare copia del software installato al fine di farne un uso personale. 5. Caricare sul disco fisso del computer o nel server documenti, giochi, file musicali o audiovisivi o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate. 6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'organizzazione. 7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'organizzazione, quali per esempio virus, trojan horses e malware in genere. 8. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte. 9. Effettuare in proprio attività manutentive. 10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell'organizzazione.

4.4. ANTIVIRUS I virus (o, per essere precisi, il malware, il software malevolo) possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, via mail … L'Istituto impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana. Il responsabile, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer e, in particolare, deve rispettare le regole seguenti: 1. Comunicare all'Istituto ogni anomalia o malfunzionamento del sistema antivirus. 2. Comunicare all'Istituto eventuali segnalazioni di presenza di virus o file sospetti. Inoltre, al responsabile: 1. È vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione. 2. È vietato ostacolare l'azione dell'antivirus aziendale. 3. È vietato disattivare l'antivirus senza l'autorizzazione espressa dell'Istituto, anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer. 4. È vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani. 9 Contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

5. SEZIONE V INTERNET

5.1. Internet è uno strumento di lavoro La connessione alla rete internet dal dispositivo avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è permesso solo relativamente alla mail e con gli accorgimenti di cui al presente documento. In particolare, si vieta l'utilizzo dei social network, se non espressamente autorizzati.

5.2. Misure preventive per ridurre navigazioni illecite L'organizzazione potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.

5.3. Divieti Espressi concernenti Internet − È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di Salute del Responsabile poiché potenzialmente idonea a rivelare dati sensibili ai sensi del Codice Privacy. − È fatto divieto di accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap. − È vietato al Responsabile lo scarico (download) di software (anche gratuito) prelevato da siti Internet; − È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto. − È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa. − È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'organizzazione, salvo specifica autorizzazione dell'organizzazione stessa. − È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica. − È vietato al Responsabile di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale. − È vietato accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dall'Istituto stesso. − È vietato, infine, creare siti web personali sui sistemi dell'organizzazione, nonché acquistare beni o servizi su Internet. Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili, è posta sotto la personale responsabilità del Responsabile inadempiente.

5.4. Divieti di Sabotaggio È vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'Istituto per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

5.5. Diritto d'autore È vietato utilizzare l'accesso ad internet, in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, D. Lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, …) se non espressamente autorizzato dall'organizzazione.

6. SEZIONE VI POSTA ELETTRONICA

6.1. La Posta Elettronica è uno strumento di lavoro L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell'articolo seguente. I Responsabili possono avere in utilizzo indirizzi nominativi di posta elettronica. Le caselle e-mail possono meglio essere assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, collaboratore, consulenza, …) proprio per evitare ulteriormente che il destinatario delle mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito. I Responsabili assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

6.2. Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica L'organizzazione è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte dei Responsabili e allo scopo prevede le seguenti misure: 1. In caso di ricezione sulla e-mail aziendale di posta personale, si avverte di cancellare immediatamente ogni messaggio, al fine di evitare ogni eventuale e possibile backup dei dati. 2. Avvisare l'organizzazione quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta, prima di aprirli.

6.3. Divieti Espressi 1. È vietato utilizzare l'indirizzo di posta elettronica contenente il nome di dominio dell'organizzazione per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'organizzazione, nonché utilizzare il dominio dell'organizzazione per scopi personali. 2. È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale. 3. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro. 4. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte. Nella definizione delle regole d'uso del servizio di posta elettronica e delle modalità di controllo, il MIUR ritiene di grande importanza salvaguardare la libertà di espressione e di pensiero e la garanzia della privacy dell'individuo. Questa Politica rispetta quindi i principi

basilari esposti, nel contesto delle obbligazioni legali e delle politiche di sicurezza dell'Amministrazione. 11 L'Amministrazione, anche sulla base delle direttive del governo tese a promuovere la crescita delle comunicazioni in formato digitale e l'abbattimento di quelle cartacee, considera la posta elettronica uno strumento fondamentale, che viene messo a disposizione di tutti coloro che ne abbiano diritto. La presente politica vale anche come informativa sulle finalità e modalità del trattamento dei dati personali, ricavabili dalle attività di controllo tecnico svolte sul servizio di posta elettronica, ai sensi dell'art. 13 della legge 196/2003.

7. SEZIONE VII GESTIONE DATI CARTACEI

7.1. Politica della scrivania pulita I Responsabili sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. I Responsabili sono invitati dall'organizzazione ad adottare una "politica della scrivania pulita". Ovvero si richiede agli responsabili di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dell'Istituto. I principali benefici di una politica della scrivania pulita sono: − Una buona impressione agli utenti che visitano il nostro Istituto.. − La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle. − La riduzione della possibilità che documenti confidenziali possano essere sottratti all'organizzazione. In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa, oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti. Prima di lasciare la propria postazione, sarà cura dei Responsabili riporre in luogo sicuro (armadio) tutta la documentazione utilizzata o prodotta durante la giornata. Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente. È necessario rimuovere immediatamente ogni foglio stampato da una stampante o dal fotocopiatore, per evitare che siano prelevati o visionati da soggetti non autorizzati. Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti. Il presente Disciplinare verrà pubblicato all'Albo Digitale e pubblicato sul sito Internet di Istituto, ai sensi dell'art. 7 della legge 300/70 e del CCNL.

Il Titolare trattamento dati

IL DIRIGENTE SCOLASTICO
Prof. Alfonso D'Ambrosio
Firma autografa omessa ai sensi
dell'art. 3 del D. Lgs. n. 39/1993