DISCIPLINARE RELATIVO ALL'UTILIZZO DEI DATI

Regole di condotta ed obblighi dei collaboratori in relazione all'uso degli strumenti informatici, di Internet e della Posta Elettronica redatto in conformità al provvedimento del Garante della Privacy (Deliberazione n. 13 del 01/03/2007 - pubblicata sulla GU n. 58 del 10 marzo 2007) comprensivo di alcune note per la gestione dei dati cartacei.

Alessandria, 1 febbraio 2022

1. SEZIONE I – AMBITO GENERALE

1.1. Definizioni

- Istituzione scolastica I.T.I.S. A Volta di seguito denominata "organizzazione"
- G.D.P.R.: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;
- D.Lgs. 196/03: Decreto Legislativo 30 giugno 2003, n. 196 novellato dal Decreto Legislativo 5 settembre 2018, n.101;
- 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;
- Lavoratore: persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito dell'organizzazione (art.2, comma 1, lettera a) del D.lgs 81/08);
- Designato: ogni lavoratore, come sopra identificato che, nell'ambito dell'attività assegnatagli, è stato autorizzato al trattamento dei dati (art. 29 del G.D.P.R. e art. 2-quaterdecies del D.lgs 196/03);
- Dispositivo: Mobile Internet Device, dispositivo mobile che può essere connesso alla rete.

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 contrattualmente richiesti.

Tali informazioni possono essere considerate, ai sensi del G.D.P.R., "dati personali" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che l'organizzazione 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 aziendale.

Ai fini di questo disciplinare si specifica, pertanto, che con il termine "dati" deve intendersi l'insieme più ampio di informazioni di cui un lavoratore 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'organizzazione 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 il designato 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'organizzazione.

Anche tra colleghi, oppure tra lavoratori 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 o da remoto attraverso l'utilizzo del computer personale espone l'ente 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'organizzazione 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 soggetti designati che si trovino ad operare con dati dell'organizzazione.

Una gestione dei dati cartacei, un uso dei computer e di altri dispositivi nonché dei servizi di 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 anche ai sensi dell'art. 13 del Codice sulla Privacy e costituiscono, quindi, parte integrante dell'informativa rilasciata agli Incaricati.

1.3. Esclusione all'uso degli strumenti informatici

All'inizio del rapporto lavorativo o di consulenza, l'organizzazione valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari dispositivi aziendali, di internet e della posta elettronica da parte dei soggetti designati.

Successivamente e periodicamente l'organizzazione 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.

Le eventuali esclusioni sono strettamente connesse al principio della natura aziendale e lavorativa degli strumenti informatici nonché al principio di necessità di cui al G.D.P.R.. Più specificatamente hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo i designati 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 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 soggetti designati ai soli fini dell'attività lavorativa.

L'organizzazione è l'unica esclusiva titolare e proprietaria 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 soggetto designato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei dispositivi aziendali o dispositivi personali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i file di filmati o altre tipologie di file) 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 designato esclusivamente per un fine di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle aziendali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare.

Qualsiasi eventuale tolleranza da parte di questa organizzazione, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

1.6. Restituzione dei dispositivi

A seguito della cessazione del rapporto lavorativo o di consulenza del designato con l'organizzazione o, comunque, al venir meno ad insindacabile giudizio dell'organizzazione della permanenza dei presupposti per l'utilizzo dei dispositivi aziendali, i designati 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 soggetto designato con l'organizzazione o, comunque, al venir meno ad insindacabile giudizio dell'organizzazione della permanenza dei presupposti per l'utilizzo di dati cartacei aziendali, i soggetti designati 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.

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, cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione possono causare gravi danni al proprio lavoro, a quello dei colleghi e dell'organizzazione 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.

L'organizzazione ha implementato alcuni meccanismi che permettono di aiutare e supportare i designati in una corretta gestione delle password, in particolare, per quanto riguarda le password di accesso al Dominio (ove previsto), è in funzione un sistema automatico di richiesta di aggiornamento delle stesse impostato dall'organizzazione secondo il livello di sicurezza richiesto dall'organizzazione stesso e, comunque, in linea con quanto richiesto dalla normativa protezione dati.

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 designati per un periodo superiore ai sei mesi verranno disattivate dall'organizzazione.

In qualsiasi momento l'organizzazione si riserva il diritto di revocare al soggetto designato 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 soggetto designato, 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[1] e numeri;

4. Le password non devono essere memorizzate nella postazione utente e su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica);

[1] Per caratteri speciali si intendono, per esempio, i seguenti: { } [ ] , . < > ; : ! " £ $ % & / ( ) = ? ^ \ | ' * - + _.

5. Le password devono essere sostituite almeno ogni sei 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 lavoratori dell'organizzazione.

In alcuni casi, sono implementati meccanismi che consentono al soggetto designato fino ad 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.

2.3. Divieto di uso

Al fine di una corretta gestione delle password, l'organizzazione stabilisce il divieto di utilizzare come propria password:

1. Nome, cognome e loro parti;

2. L'username assegnato;

3. Un indirizzo di posta elettronica (e-mail);

4. Parole comuni (in Inglese e in Italiano);

5. Date, mesi dell'anno e giorni della settimana, anche in lingua straniera;

6. Parole banali e/o di facile intuizione, ad es. pippo, security e palindromi (simmetria: radar);

7. Ripetizioni di sequenze di caratteri (es. abcabcabc);

8. Una password già impiegata in precedenza.

2.3.1. Alcuni esempi di password non ammesse

La password ideale deve essere complessa, senza alcun riferimento, ma facile da ricordare. Una possibile tecnica è usare sequenze di caratteri prive di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare (es.: "NIMzz5DICmm!", Nel Mezzo Del Cammin, più il carattere 5 e il punto esclamativo). Decifrare una parola come questa può richiedere giorni, una come "radar" meno di dieci secondi. Alcuni esempi di password assolutamente da evitare:

1. Se Username = "mariorossi", password = "mario", o ancora peggio, password = "mariorossi";

2. Il nome della moglie/marito, fidanzato/a, figli, ecc. anche a rovescio! ;

3. La propria data di nascita, quella del coniuge, ecc.;

4. Targa della propria auto;

5. Numero di telefono proprio, del coniuge, ecc.;

6. Parole comuni tipo "Kilimangiaro", "Password", "Qwerty", "12345678" (troppo facili);

7. Qualsiasi parola del vocabolario (di qualsiasi lingua diffusa, come inglese, italiano, ecc.).

2.4. La password nei sistemi

Ogni Designato può variare la propria password di accesso a qualsiasi sistema aziendale in modo autonomo, qualora il sistema in questione metta a disposizione degli Utenti una funzionalità di questo tipo (Change password), oppure facendone richiesta al Titolare. La password può essere sostituita dal Titolare, anche qualora l'Utente l'abbia dimenticata e viene gestita, dopo l'assegnazione da parte dell'amministratore, esclusivamente dall'utente.

2.5. Audit delle password

Nell'ambito delle attività riguardanti la tutela della sicurezza della infrastruttura tecnologica, l'organizzazione potrebbe effettuare analisi periodiche sulle password dei soggetti designati al fine di verificarne la solidità, le policy di gestione e la durata, informandone preventivamente i designati stessi.

Nel caso in cui l'audit abbia, tra gli esiti possibili, la decodifica della password, questa viene bloccata e al soggetto designato viene richiesto di cambiarla.

3. SEZIONE III – OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

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

3.1. Login e Logout

Il "Login" è l'operazione con la quale il designato 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 un username e una password.

In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico username e password, l'organizzazione potrà assegnare un univoco username e password per gruppi di soggetti designati 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, salvo quanto previsto dalle disposizioni contenute alla sezione 7. 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 soggetto designato 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 salvo quanto previsto dalle disposizioni contenute alla sezione 7;

4. Spegnere il PC dopo il Logout;

5. Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo dispositivo.

4. SEZIONE IV - USO DEL PERSONAL COMPUTER DELL'ORGANIZZAZIONE E DI ALTRI DISPOSITIVI (PERSONAL COMPUTER PORTATILE, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI)

4.1. Modalità d'uso del COMPUTER aziendale

Il sistema informativo aziendale è composto da un insieme di unità server centrali e macchine client connessi ad una rete locale (LAN), 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'organizzazione non effettua il backup dei dati memorizzati in locale (postazione utente).

4.2. Corretto utilizzo del COMPUTER aziendale

Il computer consegnato al soggetto designato 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, assegnata da parte dell'amministratore e successivamente gestita dall'utente, che deve essere custodita dal designato con la massima diligenza e non divulgata. Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dall'organizzazione. Per necessità aziendali, gli amministratori di sistema utilizzando il proprio 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 backup) che ai server aziendali nonché, previa comunicazione al lavoratore, accedere al computer, anche in remoto.

In particolare il soggetto designato deve adottare le seguenti misure:

1. Utilizzare solo ed esclusivamente le aree di memoria della rete dell'organizzazione 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 salvo quanto previsto dalle disposizioni contenute alla sezione 7;

3. Mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dall'organizzazione;

4. Non dare accesso al proprio computer ad altri utenti, a meno che siano soggetti designati 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 soggetto designato è vietato:

1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali del soggetto designato 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 software gratuito (freeware) e shareware prelevato dai siti internet, senza l'autorizzazione dell' Amministratore di Sistema;

4. Installare alcun software di cui l'organizzazione 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' Amministratore di Sistema. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.

5. Caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.

6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, 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 ecc.

8. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.

9. Effettuare attività manutentive in proprio.

10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell'organizzazione.

4.4. Dispositivi personali

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, dispositivi personali salvo quanto previsto dalle disposizioni contenute alla sezione 7.

Ai lavoratori, se espressamente autorizzati dall'organizzazione, è permesso solo l'utilizzo della posta elettronica aziendale sui loro dispositivi personali; è espressamente vietata la trasmissione di documenti tramite sistemi di messaggistica e/o social network.

In tal caso è necessario che il dispositivo abbia password di sicurezza stringenti e l'eventuale furto o smarrimento del dispositivo deve essere immediatamente segnalato anche all'organizzazione per eventuali provvedimenti di sicurezza.

E' vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card) e la connessione dei dispositivi multimediali quali macchine fotografiche, videocamere, tablet e smartphone.

I soggetti designati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri dispositivi personali per memorizzare dati dell'organizzazione solo se espressamente autorizzati dall'organizzazione stessa e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali dispositivi dovranno essere preventivamente valutati dall'organizzazione, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

4.5 Memorie esterne (chiavette usb, hard disk, memory card)

Ai soggetti designati può essere assegnata una memoria esterna (quale una chiavetta USB, un hard disk esterno, una memory card) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, …).

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

4.6. Utilizzo del cellulare/smartphone personale.

Durante l'orario di lavoro, comprese le eventuali pause, ai soggetti designati è concesso l'utilizzo del telefono cellulare personale ma solo per comunicazioni di emergenza o per attività strettamente collegate all'ambito lavorativo.

4.7 Distruzione dei Dispositivi

Ogni dispositivo ed ogni memoria esterna affidati agli incaricati (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), dovranno essere restituiti all'organizzazione al termine del loro utilizzo, la quale provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.

In particolare l'organizzazione provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

4.8 ANTIVIRUS

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, via mail.

L'organizzazione 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 soggetto designato, 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'organizzazione ogni anomalia o malfunzionamento del sistema antivirus;

2. Comunicare all'organizzazione eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, al soggetto designato:

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'Amministratore di Sistema 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 cd.phishing,** in particolare: non dare seguito all'apertura di file non attesi, dalla dubbia provenienza o che giungono da caselle di posta non note; non installare software sulla propria postazione di lavoro gestita, soprattutto se a seguito di sollecitazioni via email che presentino link di accesso ad altre pagine o esecuzione file; non dare seguito alla richieste di email sospette; nel caso in cui la richiesta provenga da parte del personale tecnico della nostra Amministrazione, verificare attentamente il contesto: se l'email fosse attesa, e le frasi siano scritte con grammatica e sintassi corretta, se il software di cui si richiede l'installazione abbia un fine specifico, se eventuali link nell'email puntino a siti conosciuti, se il mittente fosse noto e/o corretto. 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.

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

1. È vietata la navigazione nei siti che possono rivelare le opinioni politiche, religiose, sindacali e di salute del soggetto designato poiché potenzialmente idonea a rivelare dati sensibili ai sensi del Codice Privacy.

2. 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 e del buon costume, 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.

3. È vietato al soggetto designato il download di software (anche gratuito) scaricato da siti Internet ad eccezione del software autorizzato dall'amministratore di sistema.

4. 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.

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

6. 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.

7. 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.

8. È vietato al soggetto designato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale.

9. È vietato accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dall'organizzazione stessa e le disposizioni contenute alla sezione 7.

10. È vietato, infine, creare siti web personali sui sistemi dell'organizzazione nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.

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 soggetto designato 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'organizzazione 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 a 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 soggetti designati 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, contabilità, consulenza, …) proprio per evitare ulteriormente che il destinatario delle mail possa considerare l'indirizzo assegnato al lavoratore "privato", ai sensi dei suggerimenti del Garante a tal proposito.

I soggetti designati 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 soggetti designati 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 back up dei dati.

2. Avvisare l'organizzazione quando alla propria posta personale siano allegati file eseguibili e/o di natura incomprensibile o non conosciuta.

6.3. Divieti Espressi

1. È vietato utilizzare l'indirizzo di posta elettronica contenente il 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 redigere messaggi di posta elettronica utilizzando l'indirizzo istituzionale, diretti a destinatari esterni dell'organizzazione, senza utilizzare il seguente disclaimer: «Nota di riservatezza: Il presente messaggio, corredato dei relativi allegati contiene informazioni da considerarsi strettamente riservate, ed è destinato esclusivamente al destinatario sopra indicato, il quale è l'unico autorizzato ad usarlo, copiarlo e, sotto la propria responsabilità, diffonderlo. Chiunque ricevesse questo messaggio per errore o comunque lo leggesse senza esserne legittimato è avvertito che trattenerlo, copiarlo, divulgarlo, distribuirlo a persone diverse dal destinatario è severamente proibito, ed è pregato di rinviarlo immediatamente al mittente distruggendo l'originale.".

3. 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.

4. È vietato trasmettere messaggi a gruppi numerosi di persone senza l'autorizzazione necessaria, qualora sia necessario effettuare l'invio inserendo gli indirizzi in CCN al fine di evitare la visibilità della mailing list.

5. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.

6. 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.

7. È vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni.

6.4. Utilizzo Illecito di Posta Elettronica

1. È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.

2. È vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.

3. Qualora il designato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'organizzazione.

7. SEZIONE VII – SVOLGIMENTO DELLA PRESTAZIONE LAVORATIVA IN MODALITÀ A DISTANZA -SISTEMI IN CLOUD

7.1. Regole per il corretto svolgimento della prestazione lavorativa in modalità remota

Nei casi previsti dalla normativa vigente o da disposizioni urgenti e contingenti, i dipendenti possono svolgere la prestazione lavorativa nelle modalità del telelavoro, lavoro agile, smart working.

I dipendenti svolgono la loro prestazione lavorativa da soli, nel caso in cui si trovino in presenza di terzi (nella propria abitazione compresi familiari) dovranno adottare misure idonee per preservare la sicurezza dei dati sia in formato digitale che cartaceo. I dipendenti sono tenuti ad una condotta informata ai principi di correttezza, riservatezza, diligenza.

I dipendenti possono utilizzare dispositivi, che consentano la connessione da remoto, di proprietà dell'organizzazione o di proprietà del dipendente, idonei allo svolgimento della prestazione lavorativa al di fuori della sede di lavoro, purché siano garantiti standard che non compromettano la sicurezza dei dati dell'organizzazione. In particolare nel caso di utilizzo del pc personale (telelavoro/lavoro agile) si raccomanda di assicurarsi periodicamente:

1. che il sistema operativo della propria workstation sia aggiornato;
2. che la propria workstation sia dotata di antivirus e che questo sia aggiornato per una periodica scansione;
3. che le proprie password siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti e che afferiscono a sfera lavorativa e personale;
4. al momento della modifica delle password evitare di fare solo piccole modifiche come ad esempio numerazioni progressive ecc.;
5. di eseguire il backup periodico dei dati elaborati nell'ambito della sfera lavorativa;
6. I collegamenti internet devono avvenire tramite connessione privata (non tramite wifi aperti e pubblici).

È consentito utilizzare la casella di posta istituzionale solo per iscriversi a siti internet riconducibili alla sfera lavorativa.

È consentito al lavoratore, dietro espressa autorizzazione dell'organizzazione, la possibilità di portare all'esterno della sede scolastica la documentazione cartacea utile per l'espletamento delle proprie mansioni.

7.2. L'utilizzo del notebook, tablet, palmare e smartphone di proprietà dell'organizzazione.

Il computer portatile, il tablet, il palmare e il cellulare (di seguito denominati "dispositivi") possono venire concessi in uso dall'organizzazione ai soggetti designati, per lo svolgimento della prestazione lavorativa in modalità da remoto o per espletamento di altre attività individuate dall'organizzazione (convegni, visite in azienda, uscite, trasferte didattiche etc.).

Il soggetto designato è responsabile dei dispositivi mobili assegnati dall'organizzazione e deve custodirli con diligenza per tutto il periodo in cui si protrae la detenzione.

Ai dispositivi mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare i file creati o modificati sui dispositivi mobili devono essere cancellati in modo definitivo dai dispositivi mobili (Wiping) prima della riconsegna. Sui dispositivi mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'organizzazione. I dispositivi mobili qualora utilizzati all'esterno (convegni, visite in azienda, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei dispositivi mobili deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente l'organizzazione che provvederà – se del caso – ad occuparsi delle procedure connesse alla protezione dati e la loro eventuale perdita.

Al soggetto designato è vietato lasciare i dispositivi mobili incustoditi, sia durante l'orario di lavoro che all'esterno, in quest'ultimo caso a titolo esemplificativo: divieto di lasciare a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

I dispositivi mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciati privi di PIN.

Laddove il dispositivo mobile sia accompagnato da un'utenza, il designato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, …) e a rispettarli. Qualora esigenze lavorative richiedessero requisiti (requirements) differenti il soggetto designato è tenuto ad informare tempestivamente e preventivamente l'organizzazione.

In relazione alle utenze mobili gli utilizzi all'estero dovranno essere preventivamente concordati con l'organizzazione per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

7.3. Cloud Computing

In informatica con il termine inglese cloud computing (in italiano nuvola informatica) si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on demand attraverso Internet a partire da un insieme di risorse preesistenti e configurabili.

Le risorse non vengono pienamente configurate e messe in opera dal fornitore apposta per l'utente, ma gli sono assegnate, rapidamente e convenientemente, grazie a procedure automatizzate, a partire da un insieme di risorse condivise con altri utenti lasciando all'utente parte dell'onere della configurazione.

Quando l'utente rilascia la risorsa, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel pool condiviso delle risorse, con altrettanta velocità ed economia per il fornitore.

Utilizzare un servizio di cloud computing per memorizzare dati personali o particolari, espone l'organizzazione a potenziali problemi di violazione dei dati. I dati personali vengono memorizzati nelle server farms di aziende che spesso risiedono in uno stato diverso da quello dell'organizzazione. Il cloud provider, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti.

Con i collegamenti wireless, il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica a causa della minore sicurezza offerta dalle reti senza fili. In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per l'organizzazione, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi se il fornitore risiede in uno stato diverso da paese dell'utente.

Si ricorda che tutti i dati memorizzati nelle memorie esterne sono seriamente esposti a eventuali casi di spionaggio e appropriazioni da parte di malintenzionati.

7.4. Utilizzo di sistemi cloud

È vietato ai soggetti designati l'utilizzo di sistemi cloud non espressamente approvati dall'organizzazione. Per essere approvati i sistemi cloud devono rispondere ad almeno i seguenti requisiti:

- Essere sistemi cloud esclusivi e non condivisi;

- Essere sistemi cloud posizionati fisicamente in Italia;

- L'azienda che fornisce il sistema in cloud deve essere preventivamente nominata Responsabile al Trattamento dei dati da parte dell'organizzazione;

- L'azienda che fornisce il sistema in cloud deve comunicare all'organizzazione, almeno una volta all'anno, i nominativi degli amministratori di sistema utilizzati.

- Dovranno essere verificate tutte le indicazioni e prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul cloud.

8. SEZIONE VIII – GESTIONE DATI CARTACEI

8.1. Clear Desk Policy

I soggetti designati 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 soggetti designati sono invitati dall'organizzazione ad adottare una "politica della scrivania pulita" (clear desk policy). Ovvero si richiede ai designati di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dell'organizzazione.

I principali benefici di una politica della scrivania pulita sono:

1) Una buona impressione a clienti e fornitori che visitano la nostra organizzazione;

2) La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;

3) La riduzione 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 (per esempio per la pausa pranzo o per una riunione) sarà cura dei soggetti designati riporre in luogo sicuro (armadio, cassettiera, archivio, …) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (visitatori/ditte esterne) presenti nell'organizzazione.

A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra.

Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.

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 da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.

Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

9. SEZIONE IX - APPLICAZIONE E CONTROLLO

9.1. Il controllo

L'organizzazione, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

1. Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.

2. Evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.

3. Verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e vulnerability assessment del sistema informatico. Per tali controlli l'organizzazione si riserva di avvalersi di soggetti esterni.

Si precisa, in ogni caso, che l'organizzazione non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.

9.2. Modalità di verifica

In applicazione del principio di adeguatezza, pertinenza e limitazione di cui all'art. 5 del G.D.P.R., l'organizzazione promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili ai soggetti designati.

L'organizzazione informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

In particolare eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte dei designati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di file pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

9.3. Modalità di Conservazione

I sistemi software sono stati programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:

1. Ad esigenze tecniche o di sicurezza del tutto particolari;

2. All'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;

3. All'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

10. SEZIONE X – SOGGETTI PREPOSTI DEL TRATTAMENTO, DESIGNATI E RESPONSABILI

11.1. Individuazione dei Soggetti autorizzati

L'organizzazione ha stabilito le modalità di attribuzione delle autorizzazioni. Per quanto riguarda i soggetti preposti al connesso trattamento dei dati (in particolare, i designati alla manutenzione) sono stati appositamente incaricati di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità di sicurezza informatica, senza realizzare attività di controllo a distanza, nemmeno di propria iniziativa. I soggetti che operano quali amministratori di sistema o le figure analoghe cui siano rimesse operazioni

connesse al regolare funzionamento dei sistemi, svolgono un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

11. SEZIONE XI – PROVVEDIMENTI DISCIPLINARI

11.1. Conseguenze delle infrazioni disciplinari

Le infrazioni disciplinari alle norme del presente Disciplinare Interno potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato.

11.2. Modalità di Esercizio dei diritti

Il lavoratore interessato del trattamento dei dati effettuato mediante strumenti informatici ha diritto di accedere ai sensi dell'art. 15 del G.D.P.R. alle informazioni che lo riguardano scrivendo al Titolare dell'organizzazione e al Responsabile della protezione dei dati.

12. SEZIONE XII – VALIDITÀ, AGGIORNAMENTO ED AFFISSIONE

12.1. Validità

Il presente Disciplinare ha validità a partire da: 01 aprile 2021 ed è stato revisionato in data 01 febbraio 2022.

12.2. Aggiornamento

Il presente Disciplinare sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'organizzazione o in caso di mutazioni legislative. Ogni variazione del presente Disciplinare sarà comunicata agli incaricati.

12.3. Affissione

Il presente Disciplinare verrà pubblicato sul sito istituzionale al fine di garantirne la massima diffusione.

Il Dirigente Scolastico
Dott.ssa Maria Elena DEALESSI
(firma omessa ai sensi dell'art.3 c. 2 D.Lgs. 39/93)

Alessandria, 1 febbraio 2022